



# ADELI

La LETTRE n° 44

Juillet 2001

*Les lecteurs de la revue « Que choisir » auront sans doute remarqué dans le numéro de juin la référence à la Lettre d'ADELI n° 44, faite à l'occasion d'un article sur « les nouveaux visiteurs médicaux ». Les consommateurs que nous sommes s'intéressent désormais aux systèmes d'information. Ceci est une bonne nouvelle. Cette lettre 44 prolonge également notre réflexion sur les processus par l'annonce de l'ouverture de la commission « Maîtrise des processus » et deux articles sur la gestion de configuration. Vous y trouverez également des nouvelles du site Web et les premiers échos du dîner-débat que nous avons organisé sur le thème « modélisation et connaissance ». Bonnes vacances à toutes et à tous ! ..▲*

*Martine Otter*

La Lettre est une publication périodique d'**ADELI**, dont la coordination est assurée par **Gilles Trouessin et Martine Otter**.

Pour toute information au sujet d'ADELI :  
**info@adeli.com** ou **01.45.89.02.01**

Pour tout contact au sujet de La Lettre :  
**lalettre@adeli.com**

*ADELI*

*87 rue Bobillot - 75013 Paris - www.adeli.com*

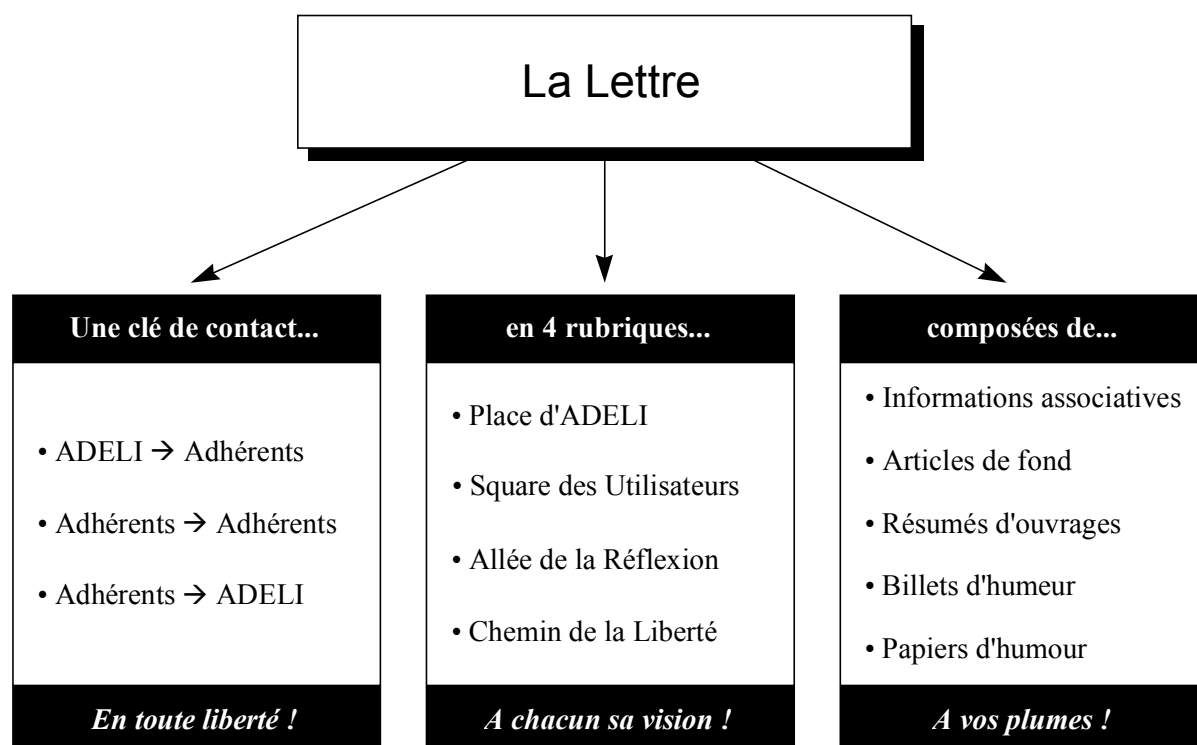
ISSN 1147-5803

©Les Éditions d'ADELI

ADELI est une association qui œuvre pour la maîtrise des systèmes d'information. Elle a été créée en 1978 et compte, à ce jour, 200 adhérents représentants d'entreprises, de SSII, d'éditeurs de logiciels ou consultants indépendants, étudiants, particuliers.

ADELI, régie par la loi de 1901, est rigoureusement indépendante de toute influence commerciale et idéologique. Ses adhérents sont des acteurs impliqués dans les systèmes d'information et concernés par les méthodes et les outils de génie logiciel. L'indépendance des travaux d'ADELI, le charisme et le professionnalisme de ses membres en font un arbitre et une référence dans le domaine des systèmes d'information. ADELI offre les conditions idéales d'une veille technologique efficace et sérieuse, qui en fait le partenaire reconnu du SYNTEC Informatique, de l'AFNOR, du CMSL et de l'AILF.

*Lien entre tous les adhérents, La Lettre propose un parcours périodique dans le monde des systèmes d'information.*



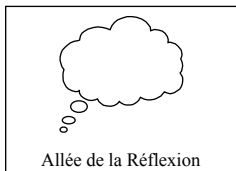
# Sommaire



<i>Le mot de la Présidente</i>	4
<i>Modélisation et connaissance</i>	5
<i>Maîtrise des processus</i>	7
<i>Des nouvelles du site</i>	9



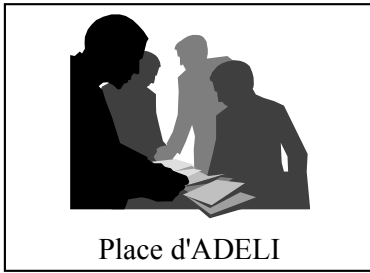
<i>Gestion de configuration :</i>	
<i>Petit guide méthodologique (1<sup>ère</sup> partie)</i>	13
<i>Gestion de configuration logiciels</i>	25
<i>Sécurité(s) et Intimité...</i>	
<i>des données à caractère personnel</i>	35



<i>Une facture d'hôpital à la veuve du donneur !</i>	45
<i>Moutons et Robots</i>	48



<i>Problème de logique : un petit casse-tête</i>	51
--	----



# Le mot de la Présidente

*Les dernières nouvelles d'ADELI*

## ADELI dans la presse

La publication du MÉTROscope a fait l'objet d'un article dans **01 Informatique** (N°1631 du 27 avril). Les lecteurs de ce numéro auront sans doute remarqué un autre article nettement plus médiatisé sur le même sujet : « Balanced scorecard : le choix des indicateurs est crucial ». La traduction française de « balanced scorecard » est tout simplement « Indicateurs et tableaux de bord », mais l'emploi de ce terme anglais non-traduit laisse entendre qu'il y aurait là une innovation majeure, ce que le dit article ne dément pas. Cet exemple vient renforcer notre intime conviction d'un besoin de démystification.

Les travaux d'ADELI sur la sécurité, animés par Gilles Trouessin, sont également cités dans le n° 383 de juin de « **Que Choisir** » qui s'intéresse à l'usage fait par les médecins des données individuelles qu'ils ont à connaître et la nécessaire confidentialité qui devrait leur être associée.

## Nouvelles commissions

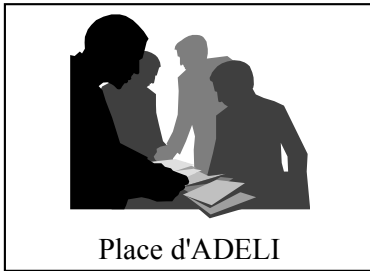
Nous vous annonçons donc dans ce numéro le lancement de la commission « Maîtrise des processus ». Le thème processus est vaste. Ces quelques extraits des messages échangés sur le forum des adhérents sont là pour le prouver :

- « Qu'est-ce qu'un processus ? »
- « Il faut, déjà, bannir le terme "Process" que certains emploient quand ils ne savent pas ce qu'ils veulent dire, en se cachant derrière un vocabulaire anglo-saxon. Il convient de distinguer le processus de la procédure en rajeunissant les définitions merisiennes qui n'étaient pas si mauvaises. »
- « La notion de processus est à rapprocher de la notion ontologique qui passe par la description d'un "objet", "élément", "être" particulier qui se voient conférer un certain nombre de possibilités de comportements. »
- « Je serais assez d'accord pour donner tout d'abord au terme processus une définition merisienne (à affiner et préciser) mais acceptée d'un commun accord comme langage commun de communication. »
- « Le processus fournit un "produit" final destiné à un "client" interne ou externe qui l'utilisera pour décider et agir. On sait que le déroulement d'un processus n'est pas linéaire ; comment l'enchaînement des activités, tâches ou opérations, va-t-il être « réglementé » ? C'est la procédure qui régleme le fonctionnement du processus. »

Là encore, il est important que nous clarifions le vocabulaire et nous livrions à un nécessaire travail de démystification.

La commission « Maîtrise de la qualité », après la sortie des nouvelles normes ISO 9000 : 2000, avait besoin de reprendre son souffle. Elle va maintenant redémarrer en s'appuyant sur les modélisations existantes des processus.

*Martine Otter*  
*Présidente d'ADELI - [president@adeli.com](mailto:president@adeli.com)*



# Modélisation et connaissance

*Dîner-débat organisé par ADELI, le 20 juin 2001*

*Ce 20 juin, veille de la désormais traditionnelle fête de la musique, Michel Demonfaucon, membre du Comité d'ADELI, a orchestré un dîner-débat sur le thème « Modélisation et connaissance ».*

*Des Adéliens et leurs invités ont tenté de répondre aux questions posées dans l'invitation : Comment la gestion des connaissances s'inscrit-elle dans la stratégie de l'entreprise ? Quels sont les impacts technico-culturels des pratiques liées à la gestion de la connaissance pour la société du 21<sup>ème</sup> siècle ?*

## La problématique

À l'aube du 21<sup>ème</sup> siècle, notre société est appelée à se transformer profondément, en organisant rationnellement le traitement de ses connaissances. Les enjeux et les impacts d'une telle transformation méritent d'être considérés au préalable, avant que ces concepts ne soient accaparés par des stratégies commerciales abusives.

- Les impacts professionnels seront fondamentaux : quels métiers privilégier pour les salariés et prestataires de demain ?
- La compétition mondiale pour l'emploi reposera-t-elle uniquement sur des compétences acquises avant l'âge de trente ans et rendues obsolètes en moins de dix ans ?
- Faut-il enfermer la connaissance dans un carcan de règles, à base de systèmes experts et de logique formelle ?
- Cette société néo-platonicienne se déchargera-t-elle de toutes ses tâches ingrates sur des robots, ou sera-t-elle amenée à maintenir l'exploitation de ressources humaines ?
- L'avantage concurrentiel d'une entreprise provient de sa capacité à innover. Comment les entreprises se différencieront-elles, si la gestion des savoirs leur apporte des résultats rigoureusement identiques ?
- Quels avantages respectifs peuvent escompter les différents acteurs de la vie économique et sociale : entreprises, administration, citoyens, consommateurs ?
- Quels seront les contrepois qui éviteront l'étouffement de l'initiative individuelle et garantiront le respect de la vie privée ?

## L'environnement du débat

Le Restaurant Le Taste-Monde d'Issy les Moulineaux a servi de cadre original à notre rencontre. Comme l'évoque son nom, ce restaurant présente une compétence distinctive. Pour accompagner les mets offerts à la gourmandise des convives, sa carte propose une gamme de vins en provenance de pays étrangers (du Chili à la Chine, en passant par les Pays-Bas et l'Afrique du Sud).

Pendant trois bonnes heures, les quinze participants ont alterné séquences gastronomiques et échanges verbaux. Sans aucun doute, la dégustation (modérée) des élixirs exotiques a développé nos esprits et délié nos langues.

Michel Demonfaucon a animé le débat, en recentrant les propos autour de thèmes communs, lorsque les conversations particulières tendaient à prendre le pas sur la discussion collective.

Voici en vrac quelques échos de ces échanges.

- Platon s'interroge sur la possibilité et sur la pertinence d'exprimer la connaissance.
- Dans la chaîne de traitement de la connaissance, ne devrait-on pas distinguer plus nettement les trois concepts complémentaires : information, document et connaissance ?
- Comment peut-on gérer des informations non structurées ?
- Trop d'informations ne tuent-elles pas l'information ?
- Comment apporter à chacun son information nécessaire et suffisante ?
- À qui appartient l'information dans l'entreprise ?
- La cession d'information s'apparente encore, pour certains détenteurs, à une perte de pouvoir.
- Toute modélisation s'accompagne d'effets pervers ; il est difficile de raisonner sans modèle, mais le modèle est souvent un obstacle à la réflexion novatrice.
- Comment maîtriser l'utilisation des moteurs de recherche ?
- Le management des connaissances concerne de plus en plus d'acteurs professionnels ; à l'instar de l'informatique des années 80, cette discipline se répand rapidement. Mais il reste une place pour les professionnels qui en maîtriseront les infrastructures.

Il est évidemment prématuré de vouloir tirer, à chaud, à l'issue de ce débat, des conclusions péremptoires définitives.

En revanche, nous avons accumulé une masse d'informations. Certains participants se sont efforcés d'enregistrer, consciencieusement, les propos qu'ils ont jugés les plus originaux et les plus pertinents.

Nous allons tenter d'ordonner ces notes et d'en exprimer les orientations. Puis, nous retravaillerons cette base pour en extraire les éléments qui enrichiront notre connaissance commune.

À suivre, une petite synthèse qui vous sera soumise dans une prochaine LETTRE.

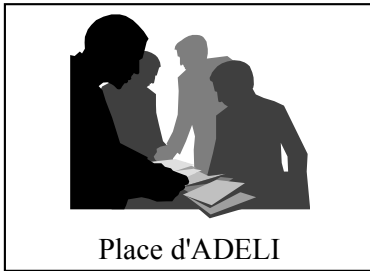
## **Renouveler une telle initiative**

Les participants présents se sont promis de récidiver, à la prochaine occasion.

Si vous souhaitez vous joindre à nous, lors d'une prochaine manifestation, faites-vous connaître auprès du secrétariat.

Indiquez-nous les thèmes de discussion susceptibles de vous intéresser. Vous serez le bienvenu.

*Le Comité*  
*info@adeli.com*



# Maîtrise des processus

## *Appel à la création de la commission*

*En septembre dernier, le Comité d'ADELI s'est concerté pour affirmer la stratégie de l'association. La maîtrise des processus s'avère être l'un des axes majeurs de notre développement.*

*Nous vous proposons d'y contribuer en participant à cette nouvelle commission « Maîtrise des processus ». Le thème de cette commission s'inscrit dans l'approfondissement des Nouvelles Technologies de l'Information et des Communications [NTIC].*

*De nombreuses entreprises sont convaincues de l'importance des processus. Mais, traditionnellement, la gestion des processus est introduite pour répondre à trois besoins :*

- *la mise en conformité aux nouvelles ISO 9000 version 2000 ;*
- *la réduction (drastique) des coûts ;*
- *et la qualité de service pour une opération de reconquête des clients.*

*Et, souvent, ces deux aspects sont mêlés dans une opération de réparation d'un préjudice.*

*En dehors de ces cas de figures, il faut reconnaître qu'il est difficile d'aborder ce thème. Certains considèrent qu'il s'agit d'une simple mode vouée à disparaître, et qu'il est impossible d'agir dans ce domaine pour toutes sortes de raisons, telles que :*

- *l'inadaptation de l'organisation : l'organisation de type matriciel, sous-jacente à la gestion des processus, irait à l'encontre de l'organisation classique que nous connaissons. Les coopérations transverses contrarieraient les habitudes d'autarcie, d'indépendance et de rétention d'information.*
- *la multiplicité des modèles et l'ambiguïté quasi générale dans l'emploi des notions de processus, de modèles de management, génère à la fois incompréhension et interprétations erronées.*

*Cette commission se propose de recueillir, d'analyser les différents modèles, outils, expériences liées à « l'approche processus ».*

## **La Commission**

### **Objectif**

Les résultats des travaux de cette commission s'exprimeront dans un ouvrage prévu pour fin 2001 et constitué des chapitres suivants :

- un glossaire ;
- l'état de l'art ;
- un panorama des approches des entreprises pour la gestion de leurs processus : chaque intervenant témoignera des méthodes et techniques utilisées dans son entreprise ;
- une analyse des retours d'expérience ;
- un état des techniques et des outils.



## **Méthode de travail**

En tout état de cause, nous privilégierons :

- la messagerie électronique, plus facile à intégrer dans un emploi du temps professionnel ;
- les présentations « vivantes » des retours d'expériences qui se révèlent toujours extrêmement motivantes pour les intervenants.

## **Comment rejoindre cette commission ?**

Si vous êtes sensibles aux approches « processus », vous pouvez enrichir votre compétence dans ce domaine, tout en apportant une contribution active.

Nous invitons tous ceux qui souhaitent rejoindre cette commission à nous contacter et à nous faire part de leurs suggestions, ce qui nous permettra d'organiser les premières présentations.

En tant que signataire de cet appel, je me propose d'animer cette commission ; vous pouvez me joindre directement par messagerie aux coordonnées indiquées sous la signature.

Ce groupe de travail constituera un carrefour d'échanges.

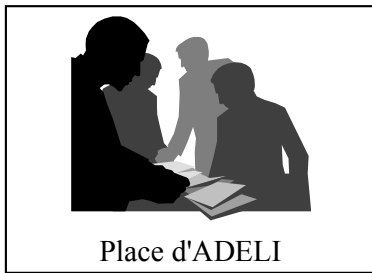
La capitalisation de ces réflexions permettra une consolidation des acquis actuels en matière de processus. Mais, on peut aussi attendre de l'analyse approfondie de ces réflexions, une élaboration d'idées concernant les principes, les méthodes et les applications des approches « processus ».

Ce groupe favorisera ainsi :

- l'enrichissement mutuel des participants, grâce à la confrontation d'expériences et aux réflexions menées en commun ;
- la diffusion des leçons tirées de ces réflexions.

Rendez-vous dans la prochaine LETTRE.

***Gina Gullà-Menez***  
***Vice-présidente d'ADELI « en charge des commissions »***  
***France Télécom R&D***  
***38/40 rue Général Leclerc***  
***92794 Issy Moulineaux Cedex 9***  
***Tél : 33 1 45 29 63 67***  
***Fax : 33 1 45 29 69 07***  
***gina.gullamenez@francetelecom.com***



# Des nouvelles du site

## *Évolutions du site Web d'ADELI*

*Notre site a évolué pour mieux répondre à vos besoins. Cet article a pour objectif d'en présenter les principales fonctionnalités et de vous donner quelques éléments statistiques sur nos visiteurs.*

## **Pourquoi consulter le site d'ADELI ?**

### ***Vous voulez en savoir plus sur ADELI***

Les rubriques du menu incontournables pour les nouveaux adhérents :

- **Présentation** : objectifs et valeurs de l'association, assortis d'un lien sur les statuts.
- **Notre Histoire** : De la programmation structurée à la maîtrise des systèmes d'information, 23 années d'histoire rapportées par notre secrétaire-trésorier et illustrées par les versions successives de notre signature.
- **Nos adhérents** : La liste des adhérents est présentée dans la partie publique du site. Vous trouverez les coordonnées précises uniquement dans la partie réservée aux adhérents. Nous comptons, bien sûr, sur vous pour ne pas utiliser une telle liste à des fins de marketing direct, ce qui serait fort peu conforme aux valeurs auxquelles vous adhérez au travers d'ADELI.

### ***Vous souhaitez participer à une commission***

Ou tout simplement avoir des nouvelles des informations sur les travaux en cours : la page **commission** vous oriente vers les différents thèmes.

Chacun des animateurs de commission est responsable de la mise à jour des informations concernant ses travaux. Nous essayons d'actualiser régulièrement ces pages, consultez-les régulièrement.

Vous pouvez également consulter la **charte des commissions** qui en précise les règles de fonctionnement.

### ***Voir les membres du comité***

Cette curiosité bien naturelle peut être satisfaite en consultant le site : nos photos sont visibles sur la page **comité** où vous trouverez également nos adresses électroniques. N'hésitez donc pas à nous contacter.

### ***Vous cherchez un article de la LETTRE***

L'ensemble des articles parus depuis le numéro 21 (octobre 1985) est référencé et a été indexé pour permettre une recherche sur mot-clé.

Les articles vieux de plus d'un an sont téléchargeables au format PDF, qui est un format compressé, à peu près universel.

Pour trouver un article sur un thème donné, utilisez le moteur de recherche que vous trouverez en utilisant la fonction Recherche du menu :

## Recherche simple

## Recherche avancée

Rechercher  dans   
 Trier par  en ordre

Vous pouvez utiliser % comme "joker".

...  
 La lettre 39 est en  
 ligne  
 ...

Par exemple, si vous cherchez CMM, vous obtiendrez ceci :

**Il y a 4 réponse(s) à votre recherche sur "CMM" dans mots clef**

Les résultats sont triés par *numéro* en ordre *décroissant*

### 1 - Améliorer les processus

Gina Gullà-Menez, Bernard Moreau - Lettre n°43 - Square des Utilisateurs - Avril 2001

Témoignage de la mise en œuvre de l'amélioration des processus liés au logiciel chez France Télécom R&D

### 2 - Le modèle COBIT

Claude Mauvais - Lettre n°43 - Square des Utilisateurs - Avril 2001

Management des technologies de l'information par les processus: Présentation du modèle COBIT

### 3 - Le modèle de maturité CMM - Mise en oeuvre et risques

Tracae Briscoe - Adaptation française par Alain Coulon - Lettre n°38 - Square des Utilisateurs - Janvier 2000

CMM (Capability Maturity Model) a été défini par le SEI (Software Engineering Institute) de l'université Carnegie Mellon. C'est un des standards de mesure de l'amélioration des processus de développement de logiciel.

### 4 - Les cinq niveaux de maturité

Alain COULON - Lettre n°22 - Allée de la Réflexion - Janvier 1996

Les entreprises vis-à-vis de la qualité et des méthodes : la classification SEI.

## Découvrir les autres publications

Elles vous sont présentées dans la page **publications**, avec quelques morceaux choisis.

Un bon de commande, sous la rubrique **commande** du menu, vous permet de passer commande des publications anciennes.

## Adhérer ?

Cette rubrique du menu ne vous concerne pas puisque vous êtes adhérent, mais vous pourriez la recommander à vos amis et collègues.

## Se retrouver entre adhérents

Nous avons créé en novembre 2000 un espace réservé aux adhérents, auxquels nous avons fourni un nom d'utilisateur et un mot de passe (n'hésitez pas à nous le réclamer si vous l'avez oublié).

Cet espace contient :

- une liste détaillée des coordonnées des adhérents ;
- les comptes rendus de nos réunions ;
- et un nouvel espace forum.

## ***Vous exprimer dans les forums***

Nous avons lancé deux forums dans les pages réservées aux adhérents :

- Processus et référentiel de connaissances,
- Qualité et maîtrise des systèmes d'information.

Ces forums sont animés par le responsable d'une commission.

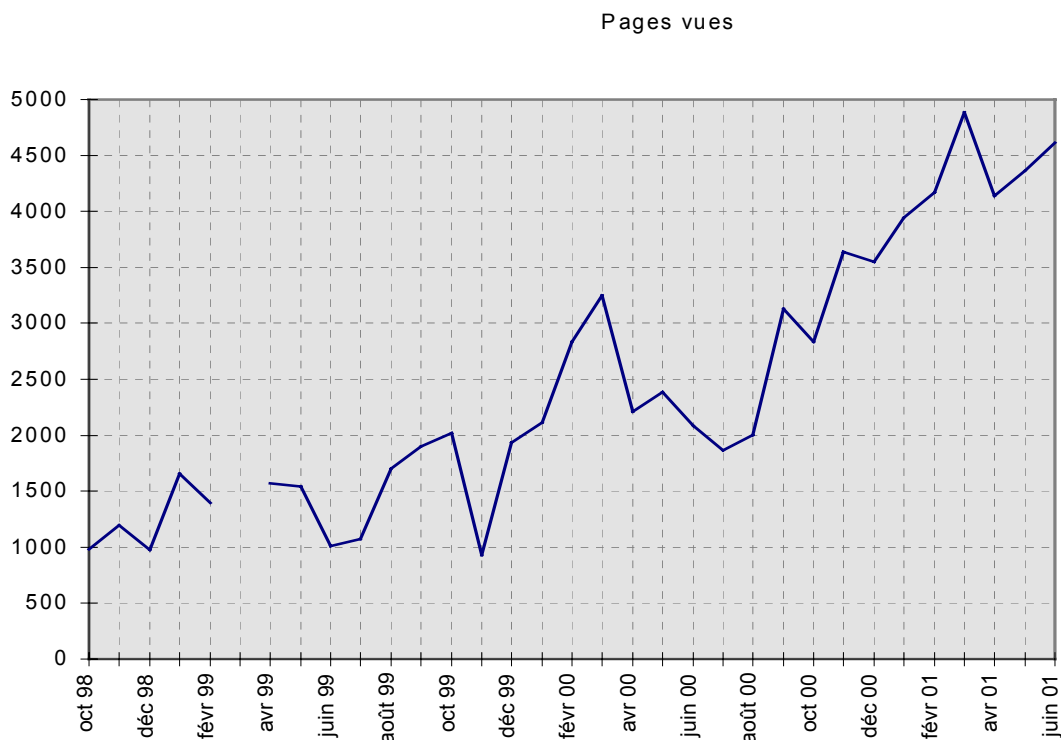
Le dialogue qui peut s'instaurer sur un forum a pour objectif de faciliter des échanges sur un mode assez informel.

Notre souhait est que le forum devienne une prolongation de chacune des commissions.

## **Quelques statistiques**

### ***Les visiteurs***

Du 1<sup>er</sup> janvier au 30 juin 2001, 3 427 visiteurs distincts ont visité notre site, certains sont revenus plusieurs fois. Au total quelques 26 117 pages HTML ont été vues, les pointes de trafic se situant autour de 16h, heure française.



Nos visiteurs sont en grande majorité français<sup>1</sup>, mais nous avons accueilli entre autre quelques belges, marocains, espagnols, canadiens, suisses, anglais, américains, sud-africains, allemands, autrichiens, japonais,...

Les moteurs de recherche Yahoo, Voilà, Wanadoo, Google, Altavista ou Lycos ont conduit vers ADELI certains visiteurs.

<sup>1</sup> Nous ne connaissons bien sûr pas la nationalité exacte de nos visiteurs, mais seulement le nom de domaine de leur fournisseur d'accès.

Des liens sur les pages de nos adhérents ou partenaires ont fait de même :

- <http://www.webinfocom.msh-paris.fr/> : Portail des sciences de l'information et de la communication, associant le Ministère de la recherche, la Société Française des Sciences de l'Information et de la Communication (SFSIC), la Fondation Maison des Sciences de l'Homme(MSH) et la librairie Tekhné,
- <http://wwwusers.imaginet.fr/~jmjaeger/cv4.html>: Site de Jean-Michel de Jaeger, ancien adhérent d'ADELI,
- <http://perso.easynet.fr/~yconstan/> : Site d'Yves Constantinidis, ancien membre du comité d'ADELI,
- <http://www-lil.univ-littoral.fr/~toffolon/>: Site de Christine Toffolon, Maître de Conférences Université du Littoral - Cote d'Opale, qui nous cite parmi ses liens préférés.

Vous pouvez bien sûr mettre également un lien vers le site ADELI sur votre page personnelle ou sur le site Internet de votre entreprise. Si vous nous prévenez de cette initiative, nous pourrions bien évidemment vous rendre la pareille. Une seule recommandation : le lien doit pointer sur la page d'accueil plutôt que sur une page quelconque du site.

### ***Les pages les plus visitées***

Ce sont par ordre décroissant :

- La liste des entreprises adhérentes : Nos visiteurs cherchent visiblement d'abord à nous situer ;
- La lettre ;
- La page de recherche ;
- Les commissions.

### ***Les 3 articles les plus téléchargés depuis le début de l'année***

Toujours par ordre décroissant :

- Le modèle de maturité CMM ;
- L'analyse de la valeur ;
- RSU 1<sup>ère</sup> partie.

## **Quelles évolutions ?**

Le site d'ADELI est votre site. Toutes les suggestions sont les bienvenues. La seule limite aux évolutions réside en fait dans le temps (bénévole) nécessaire aux mises à jour.

Si vous souhaitez participer à l'animation du site, faites-vous connaître.

***Martine Otter***  
***Présidente et Webmestre d'ADELI***  
***webmaster@adeli.com***



Square des Utilisateurs

# Gestion de configuration

*Petit guide méthodologique (1<sup>ère</sup> partie)*

*La première partie de ce guide méthodologique présente les concepts de la gestion de configuration, applicables à la maîtrise des systèmes d'information. Elle dresse un tableau des préoccupations et des enjeux. Une seconde partie, publiée dans la LETTRE 45, recensera les méthodes et les techniques utilisées par cette discipline.*

## Introduction

Une production industrielle efficace repose :

- sur la connaissance des caractéristiques des composants (matières premières et pièces élémentaires) qu'elle doit transformer et assembler ;
- sur la maîtrise des opérations qui commandent ces transformations et ces assemblages.

La **gestion de production** industrielle est l'ensemble des méthodes et des techniques qui permettent de maîtriser :

- la nomenclature des composants ;
- les gammes de fabrication.

De façon analogue, la production de systèmes d'information assemble des composants (plates-formes, progiciels, réseaux, modules de programmes, description de fichiers, langage de commande etc.).

La gestion des différents états d'un système s'appelle la **gestion de configuration**. La gestion de configuration consiste à mettre en œuvre et à utiliser des moyens organisationnels, techniques et administratifs pour obtenir, à tout moment du cycle de vie du produit, une visibilité satisfaisante du produit, au travers de ses caractéristiques physiques et fonctionnelles, généralement décrites dans des documents.

La gestion de configuration est une discipline fondamentale pour les entreprises qui développent des logiciels complexes de taille importante. Elle est incontournable pour les distributeurs de progiciels. Ces produits sont réalisés en différentes versions adaptées aux caractéristiques techniques et organisationnelles des divers sites sur lesquels ils seront installés, ce qui oblige le distributeur à maîtriser la configuration de chaque installation.

Cette gestion est rendue nécessaire par le besoin de fournir un système cohérent, quelles que soient les modifications subies par ses différents composants.

Cette gestion implique l'utilisation d'outils adaptés qui permettent de gérer, de suivre et de contrôler toutes les évolutions de chaque élément du système, en parfaite cohérence avec des normes et des règles préétablies.

On distingue deux sortes de gestion de configuration et de modifications.

- Une gestion de configuration **dynamique**, ou adaptée au **développement** permet, essentiellement, de coordonner les activités de développement des équipes, de suivre chaque composant logiciel au cours de son élaboration jusqu'à sa validation.
- Une gestion de configuration **statique**, ou adaptée à la **maintenance**, archive les composants d'un système en production, contrôle et trace ses modifications. Cette activité inclut la gestion des différentes versions du système, la gestion des sites; elle se prolonge par la gestion des livraisons, voire la gestion de la réutilisation.

Le présent document traite essentiellement le thème de la gestion de configuration en phase de développement.

## Définitions

### **Les articles composants un système d'information**

Un système d'information se compose :

- d'un ensemble de plates-formes (machines et logiciels de base) ;
- d'un ensemble de logiciels applicatifs ;
- d'une organisation décrite dans des procédures ;
- de documentations techniques et d'utilisation.

La norme ISO 10 007 : 1995 définit le terme « **article de configuration** » comme :

- un ensemble de matériels, de logiciels, de produits, issus de processus à caractère continu, de services ;
- ou un sous-ensemble défini de ceux-ci ;
- qui a été retenu pour la gestion de configuration et qui est traité comme une seule entité dans le processus de gestion de configuration.

La notion d'article de configuration est une notion gigogne. Un système se compose d'articles de configuration, eux-mêmes constitués d'articles de configuration.

Ainsi, dans le présent guide méthodologique, nous emploierons l'abréviation « article » pour désigner tout composant d'un système d'information : élément matériel, module de programme, séquence de langage de commande, document, poste de travail.

### **Les modifications d'un système**

Une modification est un changement qui n'altère pas la finalité d'un article. Les modifications jalonnent la vie du système d'information, pendant deux périodes bien différenciées.

Pendant la période de **développement**, on conçoit, on réalise et on installe le système.

Pendant la période de **production**, on exploite le système pour saisir, conserver, transformer et restituer les données nécessaires à la gestion de l'entreprise.

On peut classer les modifications selon leur origine.

- Modifications correctives en réparation d'incidents :
  - correction d'anomalies bloquantes ou majeures ;
  - améliorations mineures (présentation, lisibilité).
- Modifications évolutives demandées par l'utilisateur :
  - pour pallier un oubli ou une ambiguïté de spécification ;
  - pour s'adapter à de nouveaux besoins.
- Modifications adaptatives imposées par les contraintes des environnements :
  - pour améliorer les performances (économie de place, gain de temps) ;
  - pour s'adapter aux nouveaux environnements techniques et organisationnels.

### **Les évolutions d'un système**

Chaque modification peut entraîner une cascade de conséquences sur les différents articles qui constituent le système.

En particulier (et c'est une conséquence fâcheuse si on n'y veille pas) toute modification risque de créer des incohérences entre les articles du système. Par exemple, modifier, en urgence, un programme sans mettre à jour la documentation technique correspondante, crée une incohérence entre le programme et sa documentation.

## **Les états**

Chaque modification d'un article, aussi minime soit-elle, crée un nouvel état de cet article. Un article, en cours de transformation, passe par une séquence continue d'états consécutifs. La conservation d'états transitoires, extrêmement fugaces (modifications successives d'un module au cours de sa mise au point) ne présente aucun intérêt.

## **Les révisions d'un article élémentaire**

Certains états sont considérés comme stables : par exemple un module qualifié, testé avec succès et convenablement documenté. Ces états seront figés pour être conservés et consultés ultérieurement.

Une révision est un état d'un article dont la conservation présente un intérêt en raison de la durée prévisionnelle de stabilité de cet article. La conservation de cet état identifié (par un indice de révision) impose sa validation, son archivage (description de l'action ayant provoqué cet état, rang de cet état dans la vie de l'article, auteur, date, brève description du contexte).

## **Les branches**

On appelle branche (née d'une alternative) chaque révision indépendante issue d'une même origine (tronc). Pour identifier chacun de ces états, il faut adjoindre au concept de révision, la notion de branche. Ainsi, à un instant donné de son développement, plusieurs états concurrents d'un même article peuvent cohabiter. Il conviendra d'éviter la prolifération des branches et de procéder à des fusions pour limiter le nombre de révisions utiles.

## **Les versions d'un système**

Une version d'un système est un ensemble cohérent de révisions nécessaires et suffisantes pour répondre à un besoin prévisible. La conservation d'une version, identifiée par un numéro de version, impose l'archivage de la nomenclature des composants qui constituent cette version.

## **Les configurations d'un système**

Une configuration décrit les éléments d'un système, en précisant les différents articles composants et leurs liaisons. Elle constitue la référence d'une nomenclature d'un système, à un instant donné, en indiquant la liste des références de ses articles constituants.

Une configuration se caractérise par :

- une identification ;
- une description ;
- une liste de composants (chaque composant étant dans un indice de révision) ;
- une disposition relative de ces composants.

La gestion de configuration est la discipline qui permet de contrôler l'évolution d'un système, durant les diverses phases de développement et de maintenance et d'assurer l'intégrité et la cohérence des versions livrées. Elle met en œuvre des méthodes, des moyens et des outils qui permettent de gérer efficacement :

- l'identification ;
- la production ;
- le contrôle ;
- le suivi de l'état :
  - des constituants logiciels,
  - de la documentation,
  - des supports,
  - ainsi que de tous les outils nécessaires à leur développement et à leur exploitation.



## Le contexte de la gestion de configuration

### **Les objectifs**

Un projet d'intégration de systèmes conçoit, réalise et installe un ensemble applicatif cohérent. Chaque projet coordonne, au cours de son cycle de vie, un ensemble d'articles logiquement associés les uns aux autres.

La gestion de configuration d'un système d'information est une discipline dont les objectifs fondamentaux sont :

- l'identification des articles et de leurs relations ;
- le contrôle des évolutions de ce système durant les diverses étapes et phases du cycle de vie de développement et de maintenance ;
- la mise en place d'un processus d'archivage (révisions successives des articles et de leurs dépendances, en synchronisation avec les modifications) ;
- la traçabilité de toutes les évolutions au cours du cycle de vie ;
- la construction de versions livrables ;
- la vérification de la complétude et de la cohérence des versions livrables ;
- les éditions des rapports nécessaires à l'utilisation des différentes versions (étapes du système) à leur contrôle, au suivi d'activité.

La gestion de configuration conserve la mémoire de tout ce qui est créé, validé, avec la trace des événements déclencheurs.

La mémoire peut utiliser un support papier (documentation organisée de façon à répondre à toute question) ou un support informatique (fichiers, liens entre les fichiers, textes etc.)

Cette activité concerne les programmes (sources et éventuellement exécutables) dont le système est constitué, mais elle doit prendre en compte également :

- la documentation ;
- les manuels ;
- les procédures ;
- les enchaînements ;
- les jeux d'essais.

En résumé, la gestion de configuration doit maîtriser tous les éléments associés au système et dont il faut contrôler l'évolution et assurer la cohérence, y compris la nomenclature des éléments matériels.

### **Les enjeux**

La gestion de configuration assure une continuité d'un système, en dépit de toutes les modifications survenues au cours de sa vie, tant en développement qu'en production.

Il faut connaître l'état de chaque article, à tout instant, ainsi que son rôle dans les phases du cycle de réalisation, de façon à coordonner les phases de son développement.

Il faut être en mesure de construire, avec rapidité et sécurité, des systèmes livrables offrant les mêmes fonctionnalités sur des sites qui comportent des différences techniques (déploiement en environnement hétérogène).

Il faut pouvoir garantir la qualité des contrôles de chaque article inclus dans un système livrable.

## **Le contexte**

L'ingénierie de systèmes comporte :

- le développement (conception, construction et tests du système, mise en œuvre) de la solution ;
- le déploiement éventuel sur plusieurs sites homogènes ou hétérogènes ;
- l'exploitation ;
- la maintenance :
  - corrections d'anomalies ;
  - adaptation aux évolutions d'environnement technique ;
  - adaptation aux évolutions de l'activité de l'entreprise.

Un système est constitué d'un grand nombre d'articles de nature différente (modules de programme, description de données, documentation, jeux d'essais etc.). Ces articles possèdent de nombreuses relations, les uns avec les autres.

Plusieurs révisions successives du même article peuvent coexister :

- à un instant donné ;
- en plusieurs lieux distincts.

Le développement de systèmes d'information de grande taille, en un temps limité, appelle la collaboration d'un grand nombre de contributeurs travaillant en équipe. Ainsi, les composants du système sont construits et assemblés par des acteurs qui doivent coordonner leurs interventions autour d'articles communs.

## **La typologie des articles gérés**

Pour gérer convenablement le développement d'un système, il faut tout d'abord le modéliser par une architecture de composants reliés les uns aux autres.

Pour ce faire, on définit des articles et de règles de dépendance dont l'ensemble constitue le système résultant du développement. Toutes les méthodes de gestion de configuration proposent une telle décomposition, caractérisée par un niveau de précision et d'exhaustivité.

Malheureusement, le plus souvent, cette décomposition n'est définie qu'à partir des seuls éléments physiques tels que les fichiers les répertoires, sur lesquels sont plaqués des usages et des conventions (règles de nommages, structuration du logiciel).

Le système applicatif constitue l'essentiel d'un système d'information, sous ses différentes formes :

- modules en langage source ;
- modules exécutables (binaires générés) ;
- séquences de commande (JCL langage de commande) ;
- description des données ;
- documentation ;
  - dossier du projet :
    - ◇ plan projet,
    - ◇ plan d'assurance qualité,
    - ◇ spécifications d'objectifs,
    - ◇ spécifications externes,
    - ◇ dossier de conception technique générale et détaillée,
  - documentation technique :
    - ◇ manuel d'installation,
    - ◇ manuel d'utilisation,
- essais :
  - protocole de recette,
  - cahier de recette,
  - jeux d'essais,
  - résultats des essais,

- états des plates-formes :
  - développement,
  - exploitation.

Les articles gérés ne sont pas indépendants mais groupés en configurations de référence (ensembles complets et cohérents d'articles logiquement reliés).

Certains articles présentent des particularités.

Articles dérivés

- Un article dérivé est un article généré (quelquefois automatiquement) à partir d'un autre article (exemple code binaire généré à partir du langage source).

Articles accessoires

- Les jeux d'essais et la documentation sont des articles qui s'appliquent à d'autres articles (modules, sous-systèmes etc.).

Articles composites

- Ce sont des regroupements d'articles (par exemple, une chaîne de programmes regroupe un ensemble de programmes associés par une séquence en langage de commande).

### **Les inquiétudes**

Le chef du projet se pose les questions suivantes, relativement à la maîtrise des configurations :

- comment s'assurer de l'utilisation de l'article adéquat dans la révision souhaitée ?
- comment sécuriser cet article en garantissant son intégrité ?
- comment organiser l'évolution des articles, au cours du cycle de vie ?
- comment contrôler la cohérence de la fourniture des articles de l'application des environnements de développement vers le ou les environnements d'exploitation, cible ?
- comment suivre l'avancement de la réalisation des modifications ?
- comment connaître l'auteur de la modification ?

Il veut pouvoir répondre aux questions suivantes :

- quelle est l'identification de l'article (fichier, composant, etc.) ?
- est-il en cohérence avec les articles dépendants ?
- quelle est sa dernière révision ?
- fait-il partie de la livraison ?
- est-il mis en référentiel (archive) ?
- en existe-t-il d'autres révisions ou versions ?
- dans quel environnement doivent-ils être exploités ?
- etc.

### **Les exigences**

Il faut pouvoir identifier, sans ambiguïté, chaque article composant du système. C'est ce que l'on appelle la nomenclature.

Tous les articles doivent être identifiés :

- logiciels applicatifs, interfaces, jeux d'essais (données, JCL etc.) ;
- mais aussi les documentations de spécification, de réalisation, d'essais etc.

Mais, les articles, gérés en configuration, ne le sont pas tous de la même façon :

- les contenus de certains articles sont gérés en configuration (programmes) ;
- pour d'autres articles, des identifiants référencent des contenus gérés de façon externe (description de matériels standard).

Un premier travail doit :

- identifier les articles que l'on désire gérer ;
- définir les états qui seront conservés ;
- mettre en place une nomenclature simple.

### **Les responsabilités**

La gestion de configuration s'intègre dans le plan de développement du projet. La rigueur de gestion de configuration apparaît de plus en plus nécessaire, au fur et à mesure de l'avancement des travaux ; elle devient incontournable lors des réalisations et des premières recettes.

La gestion de configuration est l'un des constituants de l'organisation du projet ; la maîtrise des configurations relève clairement de la responsabilité du chef de projet. Cependant, pour des projets importants, le chef de projet peut déléguer cette responsabilité à un administrateur nommé chargé de la gestion de configuration.

Le même administrateur peut assurer la mission globale de gestion de configuration, tout ou long du projet ; mais, sa responsabilité peut aussi se limiter à une seule étape.

Dans la suite de ce document, nous désignerons le responsable de la fonction de gestion de configuration par le terme **administrateur**, quel que soit son statut : chef de projet ou son délégué.

## **Les solutions**

### **La place de la gestion de configuration dans un projet**

La gestion de configuration mémorise les descriptions statiques du système à chaque stade de son développement. La vision dynamique résulte d'une mise en perspective de successions de descriptions statiques dans le temps.

Chaque stade de l'évolution peut être accessible. La conservation des événements déclencheurs permet de reconstituer toute la vie du projet, de façon discontinue, au rythme des validations.

Il faut dresser l'inventaire de tous les résultats à conserver pour toutes les phases et pour toutes les étapes. Pour chaque état conservé (révision), il faut connaître :

- l'article ;
- l'auteur ;
- l'événement déclencheur ;
- la validation qui déclenche la conservation ;
- la date de conservation.

La planification fournit le descriptif des tâches et leur synchronisation, et indique ainsi :

- les états stables attendus (révisions) ;
- les événements déclencheurs (descriptifs) ;
- les liens entre toutes les révisions qui constituent une version.

La gestion des ressources, détermine :

- les acteurs et leurs fonctions ;
- les moyens techniques (supports et formes) mis en œuvre pour chaque tâche et résultat en indiquant l'ordre et lieu de rangement.

Ceci détermine :

- les poste de travail ;
- le lieu de rangement ;
  - armoire (pour les documents écrits) ;
  - bibliothèque (pour les supports informatiques) ;
- l'organisation des phases ou étapes (environnement de développement, d'intégration, de validation, d'exploitation, support externe, etc.).

La gestion de configuration doit respecter les méthodes, les normes et les standards préconisés pour le développement du système.

### **Les caractéristiques essentielles**

Chaque système est soumis à des contraintes particulières. Il répond à des besoins spécifiques, tout en respectant les usages des acteurs. Son développement et sa maintenance s'effectuent dans des environnements variés (méthodologie, technologie, management).

La gestion de configuration interagit avec d'autres activités de développement et d'exploitation de systèmes :

- conception de la solution ;
- construction et tests du système ;
- validation ;
- mise en œuvre et exploitation de la solution ;
- assurance de la qualité ;
- gestion de projet.

Les choix méthodologiques et organisationnels créent des contraintes pour la gestion de configuration et, inversement, les décisions prises concernant la gestion de configuration imposent des contraintes aux autres activités. Certains projets appliquent, des standards qui imposent des règles strictes sur la gestion des configurations, telles que :

- nomenclature d'identification des articles ;
- vocabulaire (révision, version etc.) ;
- format des documents de suivi de l'évolution ;
- normes de programmation ;
- procédures de contrôle ;
- contrôle de l'accès des utilisateurs ;
- etc.

Pour toutes ces raisons, il n'est pas concevable qu'une même gestion de configuration puisse convenir à tous les cas d'utilisation. Dès le lancement du développement, l'administrateur des configurations et des modifications doit tenir compte du degré de la flexibilité requise et des contraintes imposées, en adaptant le modèle de base.

La gestion de configuration offre les services suivants :

- reconnaissance des acteurs et gestion des accès ;
- archivage des articles ;
- gestion des révisions des articles et des versions des systèmes ;
- contrôle de la gestion du projet à l'aide de rapports détaillés ;
- traçabilité de toute l'activité grâce à une journalisation régulière des révisions et des versions, à l'édition et à l'exploitation d'historiques ;
- contrôle de la cohérence des configurations ;
- diffusion, de façon constante et reproductible, des modules en langage source pour compilation, assemblage, mise à disposition des documentations correspondantes.

## Les principales fonctions

### La gestion des espaces de développement

Les articles sont gérés en configuration tout au long de leur existence. Les développeurs façonnent des articles qui évoluent d'un état initial, embryonnaire, partiel, à un état cohérent, complet, livrable. Un article peut exister dans plusieurs espaces différents au cours de sa vie (poste du développeur, plate-forme d'intégration, plate-forme de référence, environnement d'exploitation).

Les articles et leurs dépendances sont identifiés dans la phase de préparation du projet. La phase de préparation permet de décrire les différents environnements de réalisation. L'administrateur de la gestion de configuration définit l'ensemble des moyens de mémorisation (conservation temporaire, archivage) nécessaires à la tâche correspondante et attribue des droits d'accès aux personnes habilitées. Il définit l'organisation des archives, en particulier leur taille et leur répartition physique.

Les espaces de développement communiquent entre eux lors de l'intégration et de la validation des articles : c'est-à-dire lors de la phase de construction à partir de la composition précédente. Cette communication d'information se fait par l'octroi de visibilité à certains espaces sur d'autres.

Les espaces gérés sont généralement les suivants :

- un espace de développement par développeur ;
- un espace d'intégration ;
- un espace de validation ;
- un espace de référence, qui contient tous les articles formellement validés par l'administrateur ;
- des espaces d'exploitation après déploiement.

### La gestion des articles

Un système (livrable) est un regroupement d'articles divers : programmes, documents de conception et de spécification, procédures, jeux d'essais, etc. Le système est décomposé de manière arborescente en sous-ensembles livrables qui réunissent des composants de base (modules, composants de base ou fichiers).

Il faut gérer séparément :

- la description du système et de ses articles ;
- et le contenu des articles.

La description précise la composition, l'identification et la révision de chaque article et lui associent des informations sous forme d'attributs tels que : type, état, description, date de création, de modification etc.

Les contenus des articles (programmes, textes, images etc.) sont rangés dans des archives qui contiennent les diverses révisions, les modifications successives des sources, des binaires, des documents etc., protégés contre un accès non autorisé.

La description du système peut inclure des articles **externes** dont le contenu n'est pas géré par l'outil.

Il s'agit par exemple :

- de documents qui ne sont pas sur support magnétique ;
- de programmes externes (se trouvant sur d'autres plates-formes) ;
- de composants matériels.

Une base comprend la description des systèmes gérés et les archives associées.

On considère un article commun à plusieurs versions d'un système ou, éventuellement, à plusieurs systèmes distincts, comme un élément unique.

## **La gestion des dépendances**

Les dépendances entre différents articles d'une configuration doivent être connues et prises en compte pour détecter les incohérences, et pour déterminer, à tout moment, ce qui doit être modifié pour rétablir un état cohérent.

La connaissance de ces dépendances permet de gérer la cohérence des articles entre eux ; par exemple, un code source est déclaré en incohérence dès que sa conception détaillée est modifiée, une édition de liens est mise en incohérence dès que son fichier de directives est modifié ou détruit. Ces dépendances serviront à la gestion de production.

## **La gestion des évolutions**

Lorsqu'un système évolue, il faut :

- partager des composants entre différentes versions du même logiciel, et entre différents logiciels ;
- faire évoluer une version pour créer une future livraison dérivée, à partir d'une autre ;
- permettre des modifications en cascade sur des versions successives ; par exemple, les modifications sur la première livraison doivent automatiquement être répercutées sur la livraison suivante, sachant que les deux configurations qui évoluent, sont développées, au même moment, en parallèle.

## **La gestion des modifications**

Lorsqu'un système est livré à un ou plusieurs utilisateurs, il faut respecter un processus de gestion des modifications, qui supporte le dialogue avec l'équipe de réalisation.

Une modification a l'une des origines suivantes :

- rapport d'incident - description d'une présomption d'erreur détectée à l'utilisation ;
- demande d'évolution - souhait d'évolution fonctionnelle ou d'adaptation technique ;
- en provenance de diverses sources : équipe de validation, client, utilisateurs etc.

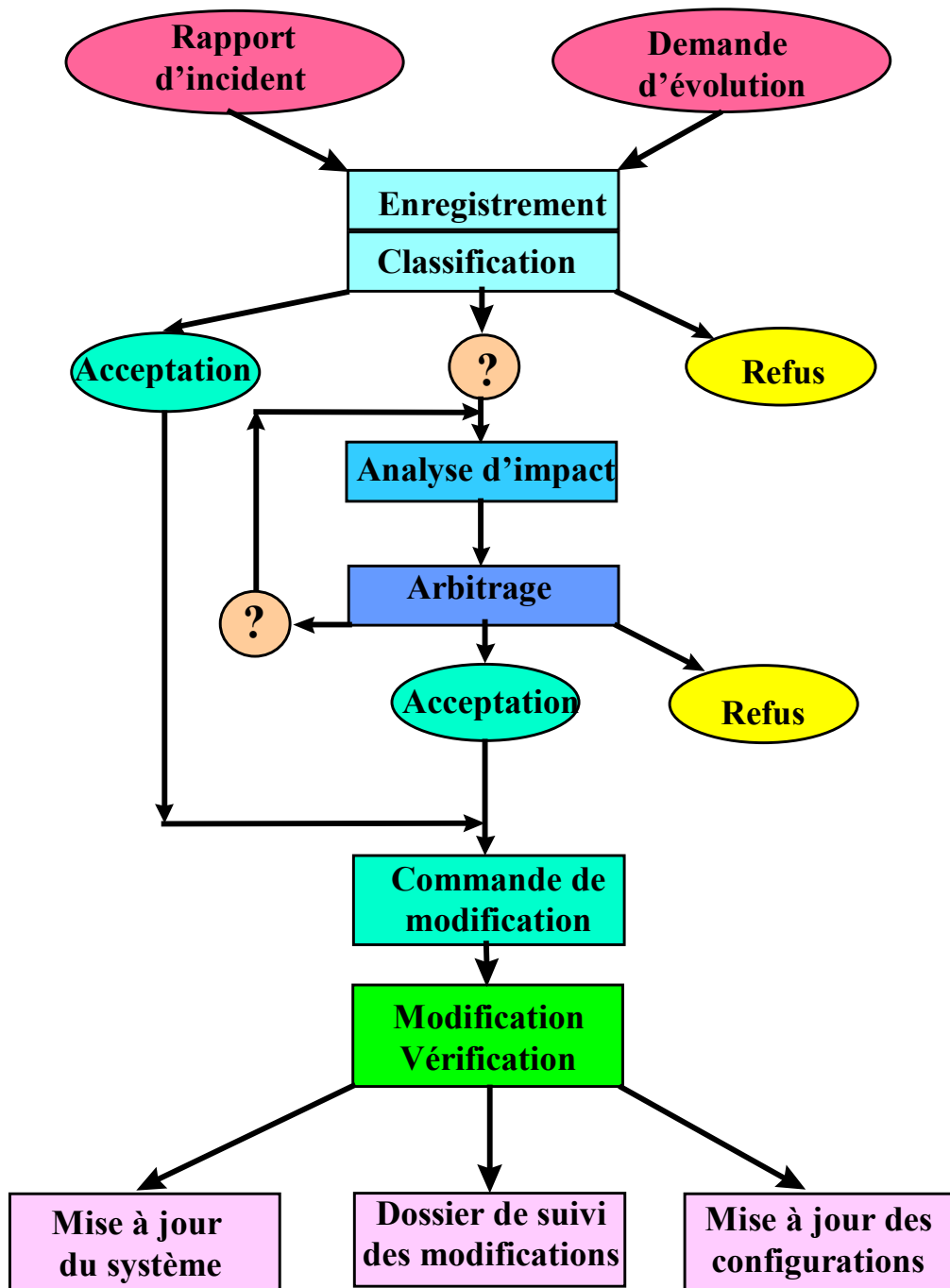
Chaque demande est analysée, évaluée (en fonction de ses impacts économiques et organisationnels) avant de décider de réaliser ou de ne pas réaliser la modification.

La prise en compte de la modification transforme la demande initiale en fiches de modification relatives aux composants concernés.

La fiche de modification décrit les modifications à effectuer ; elle est transmise à l'équipe de développement ou de maintenance qui extrait de l'archive les articles à modifier et effectue les modifications demandées. Après validation, la nouvelle révision créée est archivée.

Le dossier de suivi des modifications précise de manière détaillée toutes les modifications effectuées et décrit la nouvelle révision obtenue par différence avec la révision précédente. Il fait référence à la fiche de modification qui a déclenché les travaux.

Exemple de schéma de principe du cycle de modification d'un article





## La gestion de la production d'articles

L'administrateur met en œuvre tous les outils logistiques nécessaires pour :

- automatiser les travaux répétitifs (par exemple, en enchaînant la compilation et à l'assemblage de tous les modules du système) ;
- minimiser les manipulations (par exemple, en ne compilant que les modules rendus incohérents par la modification d'un article source ou d'une spécification) ;
- tenir compte des dépendances entre les articles pour organiser la production (par exemple les contraintes d'ordre entre modules à compiler, à assembler) ;
- résoudre les problèmes d'accès aux ressources (par exemple, les accès aux différentes bibliothèques, les accès aux outils sous licence d'exploitation, les accès aux espaces d'archivage),
- gérer les compatibilités entre outils de production (par exemple, entre les versions de compilateur, de source).

Tous les articles qui ont concouru à la production d'un autre article doivent aussi être gérés en configuration. Pour permettre de relancer une production ultérieure, il faut savoir :

- quelle version d'outil a été employée ?
- quand ?
- avec quelles options et quelles directives ?

## La chaîne de développement

La chaîne **croisée** permet d'exécuter et de tester sur la plate-forme cible destinée à l'exploitation alors que la chaîne **native** permet d'exécuter et de tester sur une plate-forme de développement distincte de la plate-forme d'exploitation.

Pendant, la chaîne native présente des avantages sur la chaîne croisée. Les développements matériels et logiciels sont souvent parallèles, la plate-forme cible qui héberge le logiciel n'est pas toujours disponible en temps voulu, en durée suffisante, pour satisfaire les besoins en ressources de l'équipement de test du logiciel.

## La génération de rapports

La gestion de configuration et de modifications des articles permet de constituer tous les rapports nécessaires au suivi. Les différents rapports d'audit et de suivi des développements, doivent être sélectifs et répondre aux normes de présentation :

- historique des modifications selon différents critères : qui fait quoi ? où ? quand ? comment ?
- journal d'activité ;
- rapport de différences entre deux versions ;
- etc.

## En pratique

Les méthodes et techniques de la gestion de configuration feront l'objet d'un article complémentaire dans la LETTRE N°45.

*Alain Coulon*  
*Secrétaire d'ADELI*



Square des Utilisateurs

# Gestion de configuration logiciels

**Comment faire mieux ce que l'on fait mal tous les jours ?**

*La gestion de configuration est l'un des 17 processus de l'ISO 12207 (processus de support du cycle de vie du logiciel). Elle figure également parmi les 24 processus d'ISO/SPICE et parmi les 34 processus du traitement de l'information du modèle COBIT (Processus de support DS 9 applicable tant aux logiciels qu'aux matériels<sup>1</sup>).*

*Une norme spécifique, l'ISO 10007 lui est consacrée. Mais tous les standards du monde sont encore impuissants à promouvoir les bonnes pratiques en la matière. Michel Demonfaucon nous dresse ici un panorama rapide de l'état de l'art.*

## Introduction

Gérer les configurations semble aller de soi. Prendre soin des objets créés ou acquis par l'entreprise relève du bon sens. Le maintien de l'outil de production en bon état de marche fait partie des règles de base unanimement respectées. Alors pourquoi s'en soucier ?

La mobilité, de plus en plus forte, des équipes ne permet pas toujours le « transfert de savoir-faire » en bon ordre. L'empilage des technologies constitue ainsi un stock de plus en plus déprécié techniquement, du fait de son non-entretien ou de sa détérioration progressive causée par des remaniements inévitables, effectués par adaptation spécifique sans reprendre en considération la globalité des objectifs de l'entreprise. Les adaptations inévitables, imposées par des contraintes extérieures à l'entreprise, faites au budget le plus bas, ou dans l'administration, effectuées au « moins-disant », c'est-à-dire au plus bas prix du marché disponible, ont des conséquences négatives sur la qualité globale du fonctionnement des systèmes.

Il faut donc passer par une gestion ordonnée des configurations. Jusqu'ici, nous parlons d'architectures très générales, le discours précédent s'applique à Beaubourg, la Tour Eiffel, le Grand Palais ou la Très Grande Bibliothèque.

La gestion de configuration est une préoccupation constante. Elle s'applique tant aux biens de l'État, qu'à ceux des particuliers (propriétaires de maisons anciennes, ceci vous intéresse lorsque vous cherchez à comprendre comment vidanger vos tuyaux posés par votre grand-père).

Le premier point à clarifier, est de définir, en tant qu'ADELI, ce qui nous semble d'intérêt pour nous. Il nous faut donc nous référer à la notion de système d'information comme objet de notre article. Ce qui forcément va nous créer des difficultés. Nous allons nous faire référence aux normes, apparues récemment dans ce domaine. Ces normes ont une portée générale. Elles sont donc à dimension paramétrable, et furtivement variable.

Pour éviter toute confusion, nous parlerons de gestion de configuration logicielle ou GCL, laissant la GC à son niveau supérieur d'abstraction.

---

<sup>1</sup> Voir La Lettre d'ADELI n°20 de février 1995 sur ISO 12207, n° 38 de janvier 1999 sur le modèle SPICE, n° 43 avril 2001 sur COBIT.

## Gestion du changement et gestion de configuration

Ces deux notions sont proches au point de se recouvrir partiellement. Pour simplifier abusivement, la gestion du changement se focalise sur les hommes, la gestion de configuration sur les choses. La gestion du changement ouvre la discussion sur la psychologie, la sociologie, l'organisation générale, et sur l'ensemble des impacts humains. Bien qu'ils restent dans le cadre des sujets adéliens, cet article ne traitera pas ces sujets<sup>2</sup>.

### Définitions

#### Gestion de configuration

*Discipline de management de projet qui permet de définir, d'identifier, de gérer et de contrôler les articles de configuration tout au long du cycle de développement d'un logiciel. (ISO 10007).*

#### Article de configuration

*Ensemble de matériels, de services ou un sous-ensemble défini de ceux-ci, retenu pour la gestion de configuration et traité comme une seule entité dans le processus de gestion de configuration. (D.Jacquin<sup>3</sup>).*

Pourquoi se restreindre au logiciel alors que le périmètre défini ci-dessus est bien plus étendu ?

Par simple souci de rester dans le cadre d'ADELI, celui du système d'information, bien que le SI soit également composé de systèmes électroniques, de réseaux, de centre de calculs, sécurisés ou non, d'immeubles de bureaux dédiés aux études informatiques, et d'acteurs divers.

Toutefois, il est évident que notre vision restrictive ne veut pas dire que la GC ne soit pas applicable ailleurs que dans le SI et autour du SI. Les normes ISO 900n-x, & ISO 10007 définissent un périmètre d'application très large et prennent en compte l'ensemble des architectures techniques, tangibles et intangibles.

## La problématique du système d'information

### **Le perfectionnisme technique**

Un simple exemple vécu montrera ce qu'il en est.

Lors d'une revue de systèmes dans une grande entreprise de services, l'on s'aperçut que l'application fournissant des données de Marketing ne pouvait plus évoluer et devait être reprogrammée en faisant appel à une version de SGBD (système de gestion de base de données) apte à intégrer des pointeurs sur des images. C'est beaucoup plus joli de montrer une belle photographie d'un produit en couleurs et tout le monde comprend de quoi il s'agit. En tout cas, c'est plus parlant que le numéro d'identification du GENCOD.

Il fut alors décidé de reprogrammer (« revamper, relooker, coloriser » !) cette application pour l'adapter à cette nouvelle version de SGBD. Le budget fut évalué et obtenu sur les bases d'une amélioration technique. Rien ne devait être changé fondamentalement à l'architecture générale permettant de fournir le service au client.

Lorsque la version du nouvel SGBD arriva, elle fut confiée au service technique pour installation. Celui-ci renvoya le produit aux études en déclarant que le système d'exploitation couramment utilisé (UNIX version  $n$ ) ne pouvait prendre en compte les « vlob » (« very large object binaries ») et qu'il était nécessaire, si les études persistaient dans leur choix, de passer à UNIX version  $n+1$ .

Ce qui fut accepté. Les services techniques revinrent alors à la charge en expliquant qu'ils ne disposaient pas d'ordinateur pouvant accepter deux versions d'UNIX à la fois et qu'il fallait acquérir un ordinateur supplémentaire. Après quelques remous, ce fût également accepté.

La nouvelle machine avec son nouveau système d'exploitation et son nouveau SGBD était là, ronronnante et prête à servir. Il suffisait maintenant de quelques travaux de changement de routines

---

<sup>2</sup> La gestion du changement a fait l'objet d'un article dans la lettre 40 : Conduire le changement – Présentation du modèle de processus de Virginia Satir – Peter de Jager

<sup>3</sup> Voir bibliographie en fin d'article.

d'appel au SGBD pour que « ça marche ». Les études se mirent à la tâche. Deux mois plus tard, la déception fut grande de constater lors d'une revue de projet qu'aucun module ne fonctionnait dans le nouvel environnement.

Il fallut commander un audit technique extérieur, et diagnostiquer les zones d'incompétences pour comprendre le dysfonctionnement du projet : le nouveau SGBD impliquait de revoir profondément la logique de déroulement des transactions, et comme le savoir-faire concernant l'application était quasiment perdu, il fallait reconstituer la logique de programmation pour modifier chaque transaction ou programme. De plus, tout cela se faisait en tâtonnant, car la formation au nouvel environnement n'avait pas été jugée nécessaire.

En quadruplant le budget initial et triplant les délais, l'affaire fut réglée. Le client, même s'il ne s'acquitta pas entièrement de l'addition, n'exprima pas réellement une grande satisfaction. Ceux qui avaient cru pouvoir conserver un poste en pratiquant mutisme et rétention de l'information ne furent pas récompensés non plus.

La nécessité de suivre, quel que soit le prix, l'évolution d'un composant due à un facteur technique exogène entraîne la refonte par montée à niveau successive de l'ensemble de l'application client. C'est l'effet Domino des architectures informatiques, qui montre bien la nécessité de procéder par ordre et avec méthode. Les études d'impact sur l'architecture, effectuées par une entité externe aux parties prenantes, auraient fortement limité les dérives en aval de ce projet, comme tant d'autres, d'ailleurs.

### **Le déni évolutif**

Il se peut aussi que vous ayez vécu une situation inverse, où tout ajout de fonctionnalité nouvelle au SI est radicalement banni pour cause de restriction budgétaire récurrente.

La logique de maintien du SI en « boîte noire » consiste à dire que ce qui fonctionne aujourd'hui ne peut que fonctionner demain. Syllogisme déjà dénoncé par Hume au sujet du lever du soleil, qui n'est assuré que par les lois de la statistique mais n'est pas une certitude absolue.

Le déni de toute évolution d'un SI conduit invariablement à rejeter de plus en plus de demandes des utilisateurs, même si elles sont fondées sur des dispositions légales nouvelles. Mais, pour les entreprises multinationales, la notion de risque inclut les risques juridiques par pays. Ce serait bien le diable que les filiales d'un groupe implanté dans 70 pays différents se heurtent toutes en même temps aux mêmes problèmes. Alors, on n'adapte plus les applications, les logiciels systèmes sont figés et reconduisent sempiternellement les mêmes bogues, que l'on finit par corriger en ajoutant une série de routines astucieuses. Comme le SI ne peut évoluer, les nouveaux utilisateurs embauchés comparent avec ce qu'ils ont vu ailleurs, et le ressentiment envers le département informatique s'amplifie. Il suffit d'une petite révolution informatique pour mettre le feu aux poudres : les ordinateurs personnels, l'interface avec écrans couleur, souris, menus déroulants, les bases de données relationnelles pour utilisateur lambda, les portables, les assistants personnels, pour enfoncer le SI dans sa spirale descendante du non-développement. Le maintien forcément régressif d'une configuration en retard technique d'évolution pour cause de restriction budgétaire amène peu à peu à la disparition du département informatique, incapable d'assumer les tâches de soutien à la gestion de l'entreprise.

### **L'objectif pour la direction de l'informatique**

L'objectif pour la direction de l'informatique consiste à faire naviguer le SI dans le chenal, bien calé entre balise verte et balise rouge. En d'autres termes, il ne faut pas se fracasser sur les rochers ni s'enfoncer dans la vase.

La gestion de configuration fait donc intégralement partie de la maîtrise du système d'information. Pour adopter un langage plus proche du terrain : « Pas de prouesse inconsidérée sans en mesurer les impacts, mais pas de stagnation suicidaire ». En reprenant les phrases de l'introduction de cet article et en l'instanciant dans le contexte logiciel, on obtient l'effet « spaghetti » pour les programmes source ou « Sicob » pour les architectures. Il faut donc planifier une évolution graduée et cohérente des composants du système et permettre cette évolution en respectant les contraintes techniques enchaînant les modifications de composant les unes aux autres.

L'exposé de cette problématique peut laisser penser qu'il ne s'agit que d'enchaînements séquentiels hiérarchisés avec des impacts, soit de bas en haut ou, inversement de haut en bas. Il existe d'autres sortes de situation : les modifications en cercle empêchant toute stabilité du système.

De même, on peut penser à des évolutions en spirale, sans fin possible. Le happening chaotique avec mouvement brownien est clairement une dégénérescence de ces modèles, caricatural mais encore bien présent, hélas. Ces états sont bien liés à la nature des systèmes logiques, il faut apprendre à dénouer le paradoxe, ou mettre fin arbitrairement à un calcul en boucle, et même pointer sur l'incohérence d'un système. L'impasse existe, bien sûr, dans cette catégorie des petits enfers possibles, ce qui est appelé en logique formelle, un système non calculable.

## **Les grands traits de la gestion de configuration logicielle**

La GCL comporte une série de choix de gestion et de conduites appropriées :

### **Inventaire exhaustif**

Il faut savoir de quoi l'on parle. La première étape consiste à recenser les objets du SI. C'est la cartographie des projets transversaux bien connus tels que AN2000 et EURO.

### **Référentiel, nomenclature et gestion des versions**

Passer de l'inventaire à une base de référence vivante et obligatoire, (seule la consultation de ce référentiel peut donner droit à l'utilisation de l'objet décrit) est une étape plus compliquée. Il faut trouver et assigner l'administrateur du référentiel et mettre en place les mécanismes d'utilisation des objets. D'autre part, se greffe sur cette utilisation la notion de nomenclature, particulièrement délicate. À ce sujet, les documents techniques (Word ou autres) doivent faire également l'objet de cette nomenclature. La nomenclature inclut la gestion des versions, qui en est une partie. Les choix de nomenclature doivent donc être concertés, documentés, testés et diffusés. L'arborescence de fonctionnement (ce que l'on voit sous l'Explorateur de Windows par exemple) fait partie intégrante des objets du SI et doit faire l'objet de référence en GCL.

### **Voies de passage**

Malheureusement, il y aura peu de chances pour que le système de GCL soit construit *ab nihilo*. Il faudra donc récupérer les existants. Chaque type d'objet devra faire l'objet d'une étude de faisabilité de récupération dans un référentiel, sinon unique, du moins unifié.

### **Pré-requis**

Chaque objet d'un SI fonctionne dans un milieu ou contexte précis. Pour chaque objet, il faudra citer ce (ou ces) contexte nécessaire au fonctionnement.

### **Modèle relationnel d'objets**

Les objets d'un SI sont en relations les uns avec les autres. C'est évident pour les tables d'une base relationnelle. Mais la hiérarchie des documents d'étude ou la référence dans un programme source de l'étude détaillée est peu fréquente. Quant aux liens entre objets de production et remontées sur les sources et leurs documentations, c'est encore plus rare sans GCL. Il faut donc veiller à créer ces liens et les gérer dans la durée.

### **Stratégies de modification**

Il faut décider de la « dureté » des blocages d'accès en mises à jour simultanées sur les objets. C'est un problème classique de l'informatique, sauf qu'ici, le blocage d'un programme source en révision peut compromettre le traitement curatif de traitement de fin de mois ou de clôture de fin d'année. Il faut donc prévoir une procédure de « percolation », c'est à dire de remontée d'autorisation dans le niveau hiérarchique pour outrepasser les blocages à impact stratégique. D'autre part, certains environnements de GCL acceptant des procédures de fusions de documents, sources, scripts ou autres, il faut décider qui peut travailler en commun avec d'autres (à deux, à trois, etc. !) ou ne pas accepter de travail en commun. En fait, il faut s'organiser en fonction du type de texte. Travailler à plusieurs sur un programme source en même temps peut sembler hasardeux, mais les documents du projet sont souvent écrits à plusieurs.

### **Simulation et génération d'impacts**

Il doit être possible avec un système de GCL de déclarer des modifications sur des objets, sans les effectuer, et d'obtenir en retour la liste ou hiérarchie des modules affectés.

## **Traçabilité des changements**

La trace de tout changement apporté à un composant doit être enregistrée sous forme d'un historique archivable. Cet historique doit pouvoir être consulté et interrogé par des requêtes.

## **Stratégies de preuves**

La stratégie de preuves est liée à celle des tests. Pourtant elle est d'un niveau supérieur, car elle fait appel à des notions juridiques de traces pouvant faire l'objet de références, notamment en termes de réception d'application et également pour audits. Ceci doit être documenté au préalable pour servir aux revues, audits internes ou externes, qui seront de plus en plus fréquents<sup>4</sup>.

## **Stratégies de déploiements**

Les déploiements sont liés à des versions d'applications, soit successives, soit dues à des spécificités de métiers ou d'environnements architecturaux. Il faut donc décider ce qui doit être géré en configuration et en mesurer l'impact sur les ressources et l'organisation.

## **Liens avec la gestion des incidents**

Le but est de rapporter au point d'origine les incidents, difficultés, inexactitudes ou arrêts en dysfonctionnement des composants de la GCL. Il est donc utile de vérifier si le « logging » des « *hot-line* » et « *help-desk* » est compatible avec les méthodes et outils choisis pour la GCL, et d'assurer qu'il existe un lien de chaînage entre incidents et composants.

L'ensemble de ces thèmes est repris dans les standards d'évolution de SI tel que les ISO 900x, ISO 10007, et par rapport au cycle de vie du projet la norme ISO 15504.

Les préconisations des normes sont couvertes partiellement et différemment selon les outils logiciels de GCL mis en place. Il faut donc faire une analyse fine des outils pour se déterminer en fonction du degré de satisfaction de norme voulue.

Indissociable de l'effort de normalisation accomplie, la GCL doit donc être située dans l'ensemble des normes fortement connexes<sup>5</sup>.

## ***Les obstacles à la gestion de configuration***

### **La problématique de l'adhésion**

Julie Kingsbury et Susan Dart<sup>6</sup> préconisent de procéder, comme pour tout projet, en cinq étapes consécutives :

1. Concertation, préparation, et planification ;
2. Définitions des processus de la GCL en fonction de l'entreprise ;
3. Évaluation des méthodes et outils par un projet pilote ;
4. Déploiement ;
5. Gestion du retour d'expérience et application des améliorations en utilisant la GCL.

### **Le curatif confinant au chaotique**

Lorsque les équipes sont constamment au front pour éteindre l'incendie, il est difficile de prendre du recul et d'améliorer les processus. D'autre part, ajouter brutalement une équipe nouvelle, souvent extérieure, ne permet pas de travailler les points utiles dans le contexte de l'entreprise. C'est donc un problème de management qui rejoint la problématique de gestion du changement évoquée plus haut.

### **L'instabilité des personnels**

C'est une situation voisine de la précédente, et souvent causée par elle. Il faut donc encourager les éléments les plus stables, leur confier plus de responsabilités si possible, et créer, peu à peu, des pôles de stabilité dans les équipes.

---

<sup>4</sup> Voir le schéma en Annexe 1 sur les revues de GCL suivant la norme 10007.

<sup>5</sup> Voir le schéma en Annexe 2 sur la structure des normes.

<sup>6</sup> Voir Bibliographie.

### **La volonté de dissimulation**

C'est la fameuse rétention d'information. On peut l'atténuer si la stabilité des personnels est assurée et si l'éthique générale du travail en équipe est respectée.

### **La crainte de la mesure de productivité**

Cette crainte doit être discutée en concertation avec ceux qui en font état. Une négociation comprenant une explication raisonnable sur l'augmentation du niveau de qualité, et des concessions sur la spécificité des situations de développement, de maintenance ou de production sera ouverte en tant que tâche du projet, si nécessaire.

### **La volonté d'anonymat**

Longtemps, les programmeurs ne souhaitent pas enregistrer leurs noms en tant qu'auteurs des programmes. Aujourd'hui, une mode inverse apparaît par les logiciels libres, où les moindres modifications de commentaire valent à leur auteur l'inscription en tant que coauteur du script ou du module, pour l'éternité de l'utilisation de la chose. Chaque environnement devra être sondé pour adopter une pratique réaliste.

### **L'incompatibilité organisationnelle**

Une très petite entreprise, employant un informaticien chargé de faire tourner quelques systèmes et des applications maison, peut à juste titre, se vouloir exemptée de GCL. Pourtant une simple application MS-Access peut comporter plusieurs bases chaînées, contenant des centaines de tables, requêtes, états et formulaires.

### **L'incompatibilité des outils**

C'est un cas de figure de moins en moins actuel, les outils étant souvent multi-systèmes et interopérables. Néanmoins, des difficultés subsistent lorsque l'architecture comprend des grands, moyens et petits systèmes, avec des systèmes d'exploitations divers. Des plates-formes logicielles d'interopérabilité existent et peuvent constituer une solution.

## ***Impacts organisationnels***

### **À quelle taille d'équipes informatiques s'adresse la gestion de configuration ?**

On s'aperçoit que toute organisation fait de la gestion de configuration comme Monsieur Jourdain faisait de la prose, sans en connaître la désignation. Cette GCL est à dimension variable et s'utilise en fonction des outils disponibles, techniquement et budgétairement.

### **En cas de dispersion des équipes de développement, la GCL est-elle applicable ?**

C'est un des objectifs de la GCL que de permettre du développement coopératif multi-sites via la gestion du développement parallèle. Cette notion est d'autant plus dans l'air du temps, que les occasions de développement « offshore » se multiplient, comme celles offertes par l'Inde, le Vietnam, la Russie, la Pologne et la Roumanie.

La gestion de configuration implique, comme tout projet, l'adhésion des acteurs :

### **Adhésion du management**

Le management de la direction informatique et de la direction générale doit être acquis et informé, et doit passer à une phase de soutien actif du projet de GCL.

### **Adhésion des exécutants**

Un effort de communication durable doit être entrepris auprès des équipes devenant les futurs utilisateurs du système de GCL.

### **Adhésion des équipes support**

Les équipes support constituent une clé du projet GCL car elles auront à charge de mettre en place les environnements adéquats de développement, intégration, réception, production et maintenance.

L'adhésion à la GCL est un projet de changement et doit être gérée en tant que telle.

## **Les types d'outils de gestion de configuration logicielle**

### **Les outils gratuits fournis avec les systèmes d'exploitation**

Ils peuvent être utilisés.

### **Les outils maison**

Ils ont un coût global élevé si l'on souhaite couvrir l'ensemble du cycle de vie.

### **Les outils du commerce**

Ils s'approchent peu à peu du paradigme souhaité.

## **Les méthodes de choix d'outils de GCL**

- D. Jacquin propose des fiches d'analyse d'outils de GCL<sup>7</sup>.
- Rational propose une méthode de choix<sup>8</sup>.
- ADELI se propose d'élaborer dans sa commission Outils de GCL un dispositif de choix. Parmi les critères à intégrer devraient figurer l'adéquation aux développements WEB, UMTS, et autres logiciels embarqués. À ce propos, un outil de GCL orienté informatique industrielle ou informatique embarquée ne donnera pas forcément de bons résultats en informatique pour applications de gestion.

## **Les coûts de la gestion de configuration logicielle**

Les coûts de la GCL peuvent représenter 5 à 10 % du coût global d'un projet. Pour certains secteurs nécessitant de très hauts niveaux de sécurité tels que l'aéronautique ou le spatial, ce coût peut atteindre 15 à 20 % par projet. Il faut comptabiliser dans le coût de la GCL la structuration de la gestion de la production si ce n'est déjà effectué, car la GCL requiert une gestion rigoureuse des espaces de développement. L'adaptation des pratiques de maintenance à la GCL peut se révéler coûteuse ou irréalisable donc contre-productive, si elle n'est pas mise en place dans la foulée des développements.

## **Les gains et avantages de la gestion de configuration logicielle**

En permettant d'établir et de valider des référentiels fiables, la GCL constitue un fondement stable de la construction et de l'évolution du SI.

- Les avantages directs se retrouvent au niveau des coûts globaux d'entretien du système. Cet apport améliore la notation CMM. Elle permet de passer du niveau 1 au niveau 3 ou même 4<sup>9</sup>.
- Les avantages indirects sont importants :
  - Confiance accordée au SI ;
  - Moral des équipes informatique ;
  - Satisfaction de la maîtrise d'ouvrage ;
  - Satisfaction des acteurs {utilisateurs, clients, directions générales} ;
  - Crédibilité des informaticiens ;
  - Détente des négociations budgétaires.

## **Conclusion**

En 1964, deux ingénieurs de la Société d'Électronique et d'Automatisme, Erström et Lalonde, ont mis au point un environnement de gestion de programmes sources, objets, données de références, résultats de derniers tests, permettant de modifier en masse à distance des applications. J'ai été chargé de faire fonctionner le produit sur SEA 3900 pour le Service de Recensement de l'Armée de Terre de la région de Valenciennes, en utilisant des machines à Courbevoie. Les résultats ont été très positifs, avec une optimisation des moyens de tests (priorités de l'époque) et un suivi statistique permettant de localiser les points difficiles et de les débloquer. La non-régression était détectée à chaque passage par comparaison des résultats nouveaux avec les résultats précédents et l'on pouvait conserver 3 versions au choix du code.

---

<sup>7</sup> Voir bibliographie.

<sup>8</sup> Voir bibliographie.

<sup>9</sup> Voir articles précédents de la LETTRE d'ADELI sur CMM.



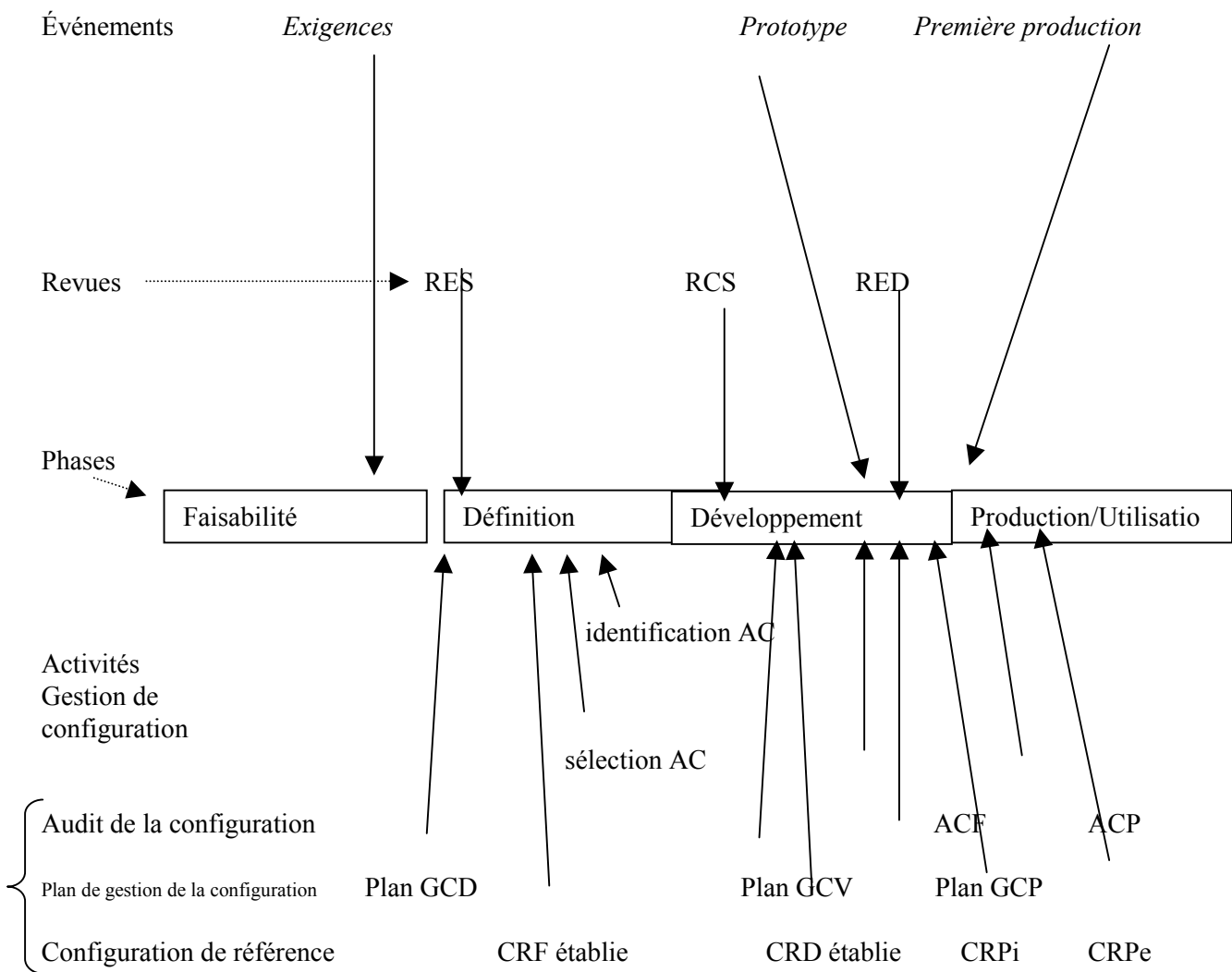
Il m'a semblé, au cours des années de projet vécues depuis lors, que peu de progrès avaient été faits. Faisons en sorte que la GCL s'applique dans l'ensemble des centres de quelque renom et sérieux. La GCL devient une partie du parcours obligé pour être qualifiable vis-à-vis de la norme ISO 9000. C'est une façon forte de proclamer le sérieux de l'entreprise dans sa conformité aux formalismes issus des bonnes pratiques érigées en lois incontournables. Il appartient aux décideurs de mettre en œuvre de tels programmes en fonction de leur chaîne de valeur.

**Michel Démonfaucon**  
**Consultant indépendant**  
**AHIMSA**

## **Bibliographie**

- ISO 9001 et développement du logiciel. Guide d'application.* ADELI-SYNTEC. Éditions de l'AFNOR-Paris La Défense. 1996. 219 p.
- Lignes directrices pour la gestion de configuration.* Management de la qualité. NF EN ISO 10007 Octobre 1996. Classement : X 50-122-7 Éditions. AFNOR. La Défense. 1996. 16 p.
- Maîtrisez votre gestion de configuration logiciel.* Dominique JACQUIN. Ed. Masson. Paris. 1996. 206p.
- Gestion de configuration logicielle : l'identification –* Éliane CUBERO. Thèse 3ème cycle. Toulouse III. 1984. 186 p.
- Proposition d'une démarche qualité logicielle pour les PME.* Régis FLEURQUIN. Thèse doctorat. INSA. 1996. 215 p.
- « *Building knowledge to prevent failure in IT development and use* ». Helena SCHEEPERS. Th. Doctorat. Aalborg U. 2000. 172 p. ISSN n° 1399-8145.
- « *Adopting SCM technology* ». Julie KINGSBURY. Software Technology Support Centre. Hill Air Force Base. Utah. 1996. <http://www.stsc.hill.af.mil/crosstalk/1996/mar/adopting.asp>. 4 p.
- « *Achieving the Best Possible Configuration Management Solution.* ». Susan A. DART. Dart Technology Strategies, Inc. California. 1996. <http://www.stsc.hill.af.mil/crosstalk/1996/mar/achievin.asp>. 7 p.
- « *Adopting An Automated Configuration Management Solution.* ». Susan A. DART. Dart Technology Strategies, Inc. California. 1994. <http://www.continuous.com/developers/developersACCE.html>. 13 p.
- Au-delà de la gestion de versions. Évaluer des systèmes de gestion de configuration logicielle.* Rational. Montigny le Bretonneux.

**Annexe 1. Phases de projet. Activités de gestion de configuration.** (norme ISO 10007).



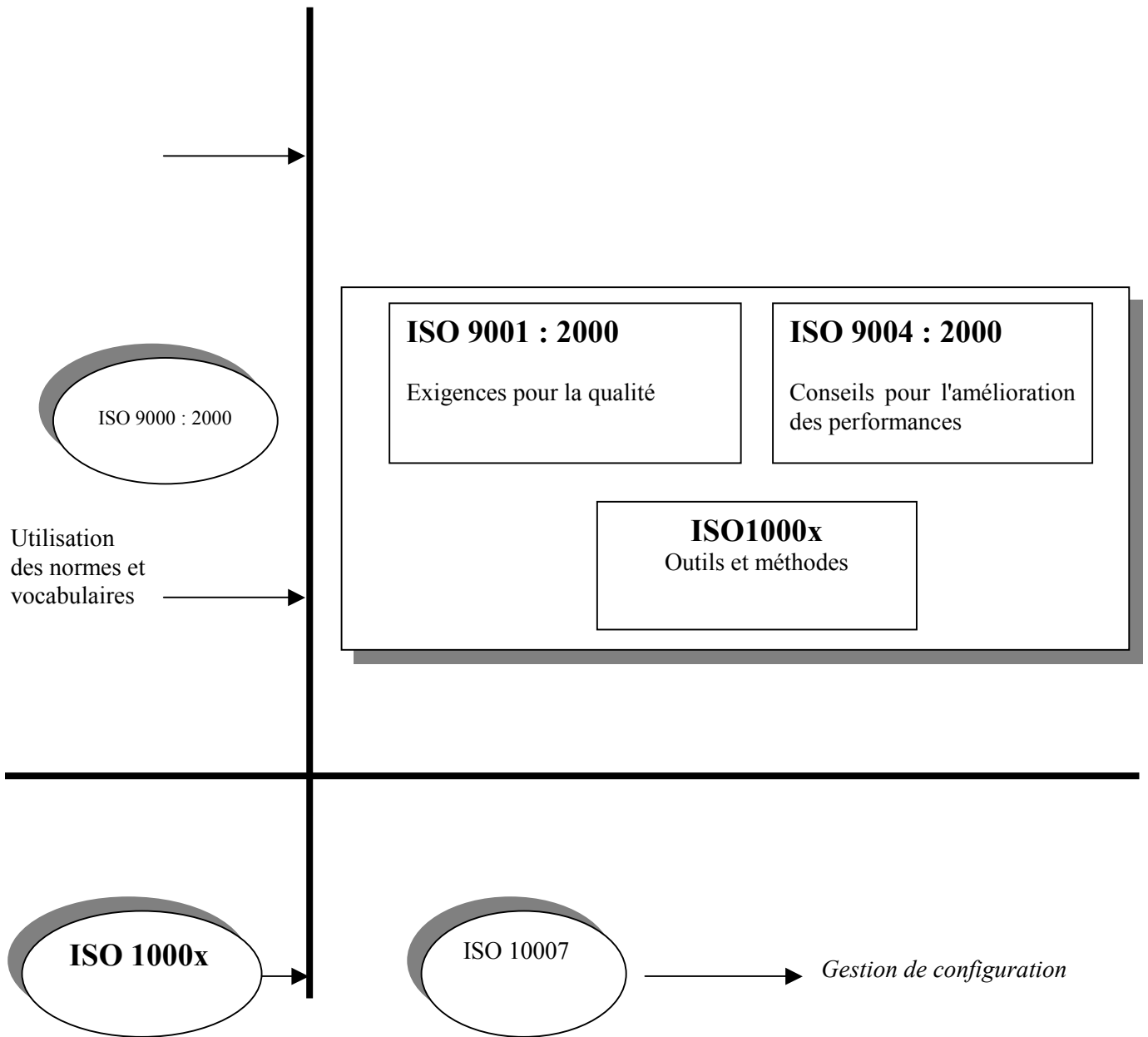
N.B. Ceci est un exemple de gestion de la configuration dans un projet donné. Si un cycle de vie de projet différent est utilisé, on peut obtenir une figure différente.

**Légende**

- CRF - Configuration Référence Fonctionnelle
- CRD - Configuration Référence Développement
- CRPi - Configuration Référence de Production initiale
- CRPe - Configuration Référence de Production établie
- RES - Revue des Exigences Systèmes
- RCS - Revue de Conception Systèmes
- RED - Revue des Études Détaillées
- ACF - Audit de la Configuration Fonctionnelle
- ACP - Audit de la Configuration Physique
- AC - Article de Configuration
- GC - Gestion de la Configuration
- Plan GCD - Plan de Gestion de Configuration en phase Définition
- Plan GCV - Plan de Gestion de Configuration en phase développement
- Plan GCP - Plan de Gestion de configuration en phase Production

**Annexe 2.**

**La structure des normes ISO 9000, ISO 9001, ISO 9004 / 2000 et ISO 1000x.**





Square des Utilisateurs

# Sécurité(s) et Intimité...

## ...des données à caractère personnel

L'article paru dans la lettre d'ADELI n°42 de janvier 2001, avait initialisé une réflexion sur la sécurité en en proposant de lever les ambiguïtés dues, entre autres, à des synonymies entre Sécurité(s) & Sûreté(s) au travers d'une présentation générale de la Sécurité, de la Sûreté et de la Sûreté de Fonctionnement des systèmes d'information. Cet article évoquait l'intimité-"privacy" qui protège la vie privée en termes assez novateurs de confidentialité-séclusion<sup>1</sup> par opposition à la confidentialité-discrétion<sup>2</sup> habituelle qui préserve le secret en des termes plus classiques et usuels. Manipuler des données à caractère personnel, pose la problématique du respect de la vie privée des individus et citoyens. Quelles spécificités peut-on, ou doit-on, ajouter à celles habituellement exprimées en sécurité des systèmes d'information ? En particulier qu'entend-t-on par :

- ...respect de la vie privée au sens habituel du terme ? S'agit-il d'intimité ?
- ...par protection des données personnelles électroniques ? S'agit-il de 'e-privacy' ?
- ...par garantie de l'anonymat le plus rigoureux possible ? S'agit-il de 'séclusion' ?

Cet article présente quelques notions sémantiques et terminologiques relatives à la sécurité, mais aussi et surtout, à l'intimité des données à caractère personnel. Telles sont, à titre illustratif mais très significatif, les données personnelles de santé/soins/médicales/hospitalières. Cet article apporte des éléments qui montrent que la prise en compte de l'intimité-'privacy' crée un métier, sinon nouveau, du moins émergent parmi ceux plus classiques et traditionnels de la sécurité informatique.

Nos exemples sont issus de la sécurité des systèmes d'information de santé, pratiquée plus de huit ans dans l'Assurance Maladie. Ce sont des besoins et de solutions qui pourront être développés et adaptés dans des secteurs connexes : médical, social, socio-sanitaire, vigilance et veille sanitaires. Ces exemples pourront être étendus à toutes les démarches que les citoyens ou communautés d'intérêts pourront mener via les nouvelles technologies de l'information et de la communication : consultations, sondages et votes électroniques, forums de discussions sur internet/web, ...

Nous ne traiterons pas les aspects purement juridiques de la sécurité et intimité des données à caractère personnel, sous-jacents à cette problématique. Il s'agit d'un métier à part entière, complexe, très précis et très rigoureux. Nous ne traiterons pas, non plus, les détails des services, techniques et outils destinés à faire respecter l'intimité-'privacy' des données personnelles électroniques.

## Introduction

Voici quelques mots-clés et expressions propres au sujet abordé que nous vous proposons d'examiner au cours de cette brève présentation.

Un dilemme, en particulier pour les systèmes d'information de santé et de soins, provient du fait qu'il faut souvent allier les deux sécurités : sécurité-'security' et sécurité-'safety'. Faut-il privilégier l'une au détriment de l'autre ? Ou, au contraire, faut-il rechercher l'équilibre ?

<sup>1</sup> 'séclusion' : mot d'origine latine (**seclusum, secludere** : séparer de). Adaptation physiologique par laquelle un animal ou une plante s'isole du milieu, empêchant passivement les actions défavorables de s'exercer sur lui. [Le Robert]

<sup>2</sup> 'discrétion' : du bas latin (**discretio, -onis** : discernement). Attitude de quelqu'un qui sait garder un secret. A la discrétion de quelqu'un : à sa disposition, à sa merci, en son pouvoir. [Le Robert]

Un élément de complication de système manipulant des données à caractère personnel provient aussi de la cohabitation entre qualité et intégrité : *qualité* des processus versus *intégrité* des données. Faut-il investir dans la qualité, voire la certification, des processus, au risque de négliger les données ?

Le manque frappant de distinction entre les formes de confidentialité à respecter pour préserver l'intimité électronique pose un problème : doit-on se contenter de respecter la confidentialité par la *discretion* (tant que celle-ci ne sera pas levée, légitimement ou non) ou peut-on obliger de la respecter par la '*séclusion*' (c'est-à-dire dès que celle-ci est instaurée, irrémédiablement) ?

Parmi les outils au service de la confidentialité, il faut rappeler la cryptographie, ou art des écritures secrètes, dont des applications récentes par rapport au classique chiffrement/déchiffrement sont : l'*occultation* des noms, l'*anonymisation* des données, la *pseudonymisation* des informations identifiantes. Pourquoi, quand, comment occulter plutôt qu'anonymiser ou pseudonymiser ?

En effet, une démarche d'occultation, d'anonymisation, de pseudonymisation peut vite devenir complexe et tout aussi sûrement inefficace si ne sont pas posées à temps les bonnes questions d'expressions de *besoins*, de réalisation d'*objectifs* et de formalisation d'*exigences*. Occultation, anonymisation et pseudonymisation pourront être *réversibles* (abus de langage), *irréversibles* (d'une manière générale), voire *inversibles* (dans certaines situations précises). Comment décider ?

On pourra parfois répondre à des exigences de *chaînages* (entre données anonymisées) mais aussi à des exigences de *robustesse* (des identifiants anonymisés ou pseudonymisés). Que faut-il choisir ?

**Exigences de chaînage** : si les techniques de *fragmentation* des fichiers et de données répondent utilement à des soucis de type *confidentialité-discretion*, la technique de *segmentation* des liens de chaînage entre données anonymes répond parfaitement à un souci de *confidentialité-séclusion*, tout en respectant, précisément, les exigences de chaînage acceptables et légitimes.

**Exigences de robustesse** : ces exigences doivent faire face aux risques de *désanonymisation directe* (cryptographique), *indirecte* (procédurale) ou par *inférence* (en logique) d'informations nominatives à partir de données non nominatives, en cas de trop grande corrélation d'informations.

## Sécurité(s) des données à caractère personnel : développements

### Rappel du trio sécurité : aspects juridiques-procéduraux-techniques

Dans la lettre n°44 d'ADELI de janvier dernier, nous avons introduit le trio de la sécurité :

- *responsabilité* des acteurs ou composante *juridique* ;  
(qui est responsable de, et pourquoi, mettre en oeuvre la sécurité ?) ;
- *superstructure* organisationnelle ou composante *organique* ;  
(où, quand, faut-il, peut-on, doit-on sécuriser le système ?) ;
- *infrastructure* opérationnelle ou composante *technique* ;  
(comment faire et faire en sorte de mettre en oeuvre la sécurité ?).

Que ce soit en sécurité- '*security*' ou en sécurité- '*safety*' :

- des aspects juridiques orientent tout d'abord les décisions et les actions, telles que, l'obligation de confidentialité et d'intégrité des données à caractère personnel, faite par la loi Informatique et Libertés ou la directive européenne sur la protection des données ;
- puis des aspects organisationnels mettent ensuite ces décisions en applications ; par exemple, la séparation des rôles et des pouvoirs et habilitations interdisant la rencontre, dans des systèmes médico-financiers ou médico-administratifs, entre d'un côté des données purement médicales, de type diagnostics ou pathologies, et d'un autre côté l'identifiant national des personnes servant de numéro dit, abusivement, « de sécu. » ;
- et enfin des techniques, telles que le contrôle d'accès aux informations ou la cryptographie dans les échanges électroniques, les réalisent concrètement.

## **Le dilemme Sécurité-Sûreté en santé**

Deux formes de sécurité sont souvent amenées à cohabiter, en particulier dans des systèmes ou applicatifs critiques manipulant des données de santé, donc à caractère personnel :

- *Sécurité-"security"* : dans la mesure où les données personnelles manipulées doivent être rendues suffisamment disponibles, intègres et confidentielles pour être considérée comme 'de confiance', ou authentiquement crédibles, mais aussi être parfaitement auditables ;
- *Sécurité-"safety"* : dans le sens où certaines données, parfois anodines telles que celles relevées et rendues accessibles par une infirmière ou une aide-soignante, sont cruciales, en termes de pertinence et de fiabilité pour la santé, voire l'innocuité, du patient ou du malade.

La '*security*' répond aux exigences fonctionnelles et apporte les solutions *ad hoc* comme les politiques d'autorisation ou interdiction, à accéder, modifier, lire des informations. La '*safety*' impose des contraintes particulières et procédures spécifiques, comme le partage d'information, pour donner pleine confiance dans la réactivité et la sûreté du système de soins et de ces différents processus.

Ainsi, on doit trouver un juste milieu entre trop de confidentialité au prétexte du respect de la vie privée et trop peu de confidentialité pour des soucis de partage efficient d'information. Ici se place utilement le débat entre confidentialité-*discrétion* et confidentialité-*séclusion*, et aussi entre '*security*' et '*safety*' d'une manière générique.

### **Sécurité(s) par la disponibilité**

À quel niveau doit-on placer l'exigence de disponibilité de l'information de santé ou de soins, dans le contexte des établissements/structures délivrant des soins ou devant prendre des décisions vitales ?

Trop d'exigences de disponibilité coûte très cher et ampute d'autant les efforts consentis sur les autres aspects de la sécurité ou sur d'autres composantes du système d'information. Mais, c'est parfois la donnée la plus anodine qui peut permettre de construire un diagnostic critique ou sérieux. On souhaiterait donc disposer, toujours et partout, de l'information utile et pertinente.

À l'inverse, trop peu d'exigences de disponibilité, paralyse un système insuffisamment opérant, voire totalement inopérant. Le système d'information se réduit alors à un simple système informatique, incapable de fournir en temps utile les éléments d'information décisifs et/ou les processus de décision, eux-mêmes. Dès lors qu'il s'agit de système vital, ce n'est pas acceptable.

Un juste équilibre de la politique de disponibilité et une bonne opérationnalité de celle-ci contribuent à la fois à la sécurité- '*security*' et à la sécurité- '*safety*'.

### **Sécurité(s) par l'intégrité**

À quel niveau placer l'exigence d'intégrité des données de santé ou de soins, dans le contexte des établissements et structures des soins. Les systèmes d'aide aux décisions autour des politiques socio-sanitaires, dans les caisses maladie, vieillesse, famille (nationales, régionales, voire locales) ont aussi besoin d'information suffisamment intègres, implicitement précises et correctes, pour travailler en toute pertinence, mais au détriment parfois du respect de la vie privée des assurés sociaux et des malades.

En effet, trop d'exigences d'intégrité ont pour incidence, par exemple, de gérer une masse faramineuse de détails informationnels, sous prétexte de pouvoir en avoir besoin le moment venu. Rappelons que c'est parfois la donnée la plus anodine qui peut permettre de construire une démarche sanitaire ou sociale pertinente car équitable et juste à temps. On entre dans des débats du style : précision *versus* pertinence, correction *versus* fraîcheur, qualité *versus* fiabilité des données.

A l'inverse, un système conçu avec trop peu d'exigences d'intégrité serait de mauvaise qualité et peu efficace, ce qui est inacceptable lorsque sont manipulées des données médicales vitales ou critiques pour la santé des patients, ou critiques ou sensibles pour l'estimation de l'état sanitaire d'une catégorie de population, ou pour un espace-temps ou un périmètre géographique et/ou thématique donné.

Un juste équilibre de la politique d'intégrité et une bonne efficacité de celle-ci contribuent à la fois à la sécurité- '*security*' et à la sécurité- '*safety*'.

## Sécurité(s) par la confidentialité

Pourquoi et comment gérer la confidentialité dès que l'on touche à des données à caractère personnel, notamment des données de santé ? L'Ordre National des Médecins rappelle que toute donnée de santé, dès lors qu'elle est connue d'un médecin, devient secret médical. Le secret médical est un secret professionnel « d'ordre public », ce qui veut dire que même le malade ou le patient ne peut délier son propre médecin du secret médical le concernant.

Il faut être très prudent et professionnel pour conseiller, décider et mettre en oeuvre des solutions de sécurité par la confidentialité. Une subtilité s'impose désormais pour distinguer deux notions appelées respectivement confidentialité-*discretion* et confidentialité-*séclusion* :

- *discretion*<sup>3</sup> : ce terme désigne la notion de ce qui est confidentiel, bien évidemment, et secret. Le secret en question, et par suite la discrétion y afférant, pourrait être levé dans des conditions qui doivent être précisées en vertu du trio sécurité déjà évoqué : conditions juridiques (légal, réglementaires), organisationnelles (par qui, sur ordre de qui ?), techniques (selon quelle méthode, protocole, technique, outils, algorithme ?) ;
- *séclusion*<sup>4</sup> : ce terme désigne une notion qui traduit la volonté de rester reclus dans son intimité (électronique, en l'occurrence). Forme de réclusion active, par choix délibéré et non pas par force (comme le laisserait entendre le terme '*réclusion*') la '*séclusion*' est un droit de chacun en vertu, là encore, de conditions issues du trio sécurité évoqué *supra* : conditions juridiques (cf. loi Informatique et Libertés de 1978, directive européenne sur la protection des données personnelles de 1995, ...), organisationnelles (quand et où garantir la vie privée des individus, en version 'données personnelles électroniques'), techniques (comment et avec quel degré de confiance et de robustesse garantir un anonymat, par exemple).

Par analogie avec les arguments formulés dans les deux paragraphes précédents, '*sécurité par la disponibilité*' et '*sécurité par l'intégrité*', trop ou pas assez de confidentialité serait nuisible au système ; trop ou trop peu de confidentialité conduit à paralyser l'utilité du système ou de l'applicatif :

- par exemple, interdire tout accès aux données nominatives à des utilisateurs dont le métier est de manipuler de telles données pour rendre un service à l'utilisateur directement, serait inutile et inapproprié ; de même, utiliser la cryptographie coûteuse en temps de calcul (voir ci-dessous chiffrement asymétrique) pour échanger de gros volumes de données, serait paralysant et tout aussi inapproprié ;
- à l'inverse, accorder un accès universel à l'information nominative par manque de discernement aboutirait à une perte de confiance totale dans le système, à son rejet et à sa non-utilisation. Refuser tout recours à de la cryptographie, dont le chiffrement symétrique, au seul motif que c'est une technologie intrinsèquement complexe ou *a priori* coûteuse, sans plus analyser les besoins, serait un manque de sérieux manifeste et conduirait à une méfiance compréhensible.

On découvre, ici aussi, qu'une mauvaise option de confidentialité serait nuisible au système et à la confiance qu'il inspire. Faire appel à la confidentialité-*discretion* en lieu et place de la confidentialité-*séclusion* ne permettrait pas de répondre à une attente de respect de la vie privée ou, inversement, mettre en œuvre la confidentialité-*séclusion* en lieu et place d'une confidentialité-*discretion* ne permettrait pas au système répondre aux fonctionnalités attendues :

- par exemple, chiffrer les noms des patients, dans une application d'accès à des bases de données statistiques sur les consommations de soins permettrait de masquer de façon seulement transitoire, c'est-à-dire '*occulter*', les noms des patients. Un utilisateur de cet applicatif, ayant accès à la fonctionnalité de déchiffrement, pourrait déchiffrer les noms des patients, alors que son métier de statisticien ne le légitime pas pour cela. Il s'agit avant tout de garantir la

---

<sup>3</sup> La *discretion*, dont une traduction pertinente en anglais est '*secrecy*' (ce qui est secret), correspond à la cryptographie dite '*à clé secrète*', car cette clé secrète de chiffrement est partagée entre l'émetteur et le récepteur d'un message (en général).

<sup>4</sup> La *séclusion*, dont la traduction immédiate en anglais est '*to seclude*' et une traduction plus indirecte, mais en cohérence avec la *discretion*-'*secrecy*', sera plutôt '*privacy*' (ce qui est du ressort de la vie privée), correspond cette fois à la cryptographie dite '*à clé privée*', en ce qu'une clé de signature (en général), et parfois de chiffrement, est et doit demeurer privative à son propriétaire et détenteur afin qu'il en soit le seul et unique maître et donc seul et authentique utilisateur.

séclusion et non pas d'apporter une certaine discrétion, car gérer des statistiques anonymes ne doit pas permettre de retrouver un patient, car il ne s'agit pas là de lui apporter des soins ;

- à l'inverse, utiliser des techniques d'anonymisation remplaçant les noms des patients par des numéros plus ou moins aléatoires définitifs et irréversibles, dans un logiciel de gestion de cabinet médical, par exemple, garantirait définitivement et irrémédiablement l'anonymat électronique des patients du cabinet. Mais, on ne pourrait reconnaître les noms ou identités des individus, ainsi répertoriés inutilement. Dans ce cas, il s'agit d'assurer une certaine discrétion dans la gestion des dossiers médicaux ; cette discrétion doit être levée par le médecin, en cas de besoin, ce logiciel de gestion de dossiers médicaux doit précisément de permettre d'accéder aux dossiers médicaux nominatifs, afin de participer au protocole de soins et de favoriser ainsi la continuité des soins.

### **Sécurité par l'auditabilité**

Pour l'auditabilité, il faut obtenir un bon compromis entre perfection et efficacité. L'auditabilité, bien que moins connue et moins pratiquée des quatre propriétés de base de la sécurité est la plus transversale et la plus fondamentale. On recommande, tout particulièrement, son application à tout système d'information d'une sensibilité particulière. Tel est le cas fréquent des systèmes d'information de soins et de santé, lorsqu'il faut fournir à la justice des preuves du bon fonctionnement et de la bonne utilisation du système d'information.

Sans entrer dans des détails élaborés ou fastidieux à ce point de notre réflexion sur la sécurité, il nous faut donner un aperçu clair de ce que l'on entend par '*sécurité par l'auditabilité*' pour ensuite l'aborder utilement sous l'angle de la '*sécurité et intimité des données à caractère personnel*'.

Résumons simplement l'auditabilité<sup>5</sup> d'un système d'information à « sa capacité à fournir en temps et lieu et en forme et fond, les éléments probants nécessaires à la démonstration de son bon fonctionnement et de sa bonne utilisation », c'est-à-dire :

- *capacité* : l'aptitude à être auditable doit être spécifiée, développée et intégrée au système et mise en œuvre de façon opérationnelle ; l'auditabilité se construit au tout premier stade de l'élaboration du système et se poursuit tout au long de son cycle de vie ;
- *en temps et lieu et en forme et fond* : la preuve devra être construite en fonction du contexte d'utilisation du système, de son utilisation probable ou présumée et donc à partir des éléments électroniques probants y afférant, qui devront, par conséquent, être accessibles (cf. *en temps*), accédés (cf. *en lieu*), mais exploitables (cf. *en forme*) et exploités (cf. *en fond*), devant toute instance nécessitant de s'en saisir pour apprécier la réalité de la situation ;
- *les éléments probants nécessaires* : il s'agit des éléments de trace des actions effectuées sur (cf. '*traçabilité*') ou menées par le système et à la suite de l'imputation de celles-ci à leurs auteurs (cf. '*imputabilité*'), mais aussi, le cas échéant, les éléments *a priori* opposables devant un juge (cf. '*opposabilité*') et donc les éléments *in fine* acceptés comme irréfutables<sup>6</sup> lors du jugement (cf. '*irréfutabilité*') ; on se situe ainsi à la frontière entre la technique et le juridique ;
- *la démonstration de son bon fonctionnement et de sa bonne utilisation* : une démonstration superficielle apporte quelques éléments d'assurance et donc de confiance dans la sécurité du système. Une démonstration plus approfondie utilise une démarche plus formelle : scientifique et/ou juridique : un cheminement rigoureux parcourt les points fondamentaux du droit qui imposent de démontrer l'engagement et donc le respect des responsabilités de chacun des contributeurs au fonctionnement et à l'utilisation du système : commanditaire, spécificateur, concepteur, développeur, intégrateur, testeur, valideur, recetteur, opérateur d'exploitation, utilisateur final,...

L'auditabilité des données à caractère personnel fait apparaître la nécessité de considérer d'autres éléments de confiance indispensables, voire primordiaux pour reconnaître la légitimité et la sincérité des systèmes d'information manipulant des données personnelles.

En voici une liste certes non exhaustive :

---

<sup>5</sup> La norme européenne expérimentale "ENV13608-1 : Security for healthcare communications – Concepts and terminology" fournit une définition consensuelle de l'auditabilité, suffisamment générique pour être applicable hors du secteur santé.

<sup>6</sup> Les juristes se permettront d'utiliser des termes comme irrévocable (action) ou irréfutable (décision).



- qui définit la politique de collecte, de traitement et d'utilisation des informations nominatives ?
- comment est développée la politique d'occultation, d'anonymisation, de pseudonymisation,... ?
- qui est en charge d'appliquer, de faire appliquer, ou de faire respecter les techniques d'occultation, d'anonymisation, de pseudonymisation ?
- comment est authentifié un individu statistique dans une base de données statistique ?
- qui peut attester de l'identification d'une personne physique parmi une population ?
- qui peut répondre de la fiabilité du processus d'identification des individus d'une population ?
- pourquoi et comment choisir entre confidentialité-discrétion et confidentialité-séclusion ?
- pourquoi, quand et comment lever la discrétion sur des données à caractère personnel ?
- qui doit se porter garant de l'occultation des noms de l'anonymisation de données ou de la pseudonymisation d'identifiants ?
- comment garantir la qualité et l'exhaustivité d'informations anonymisées ?
- comment appliquer l'auditabilité à des systèmes d'information non entièrement auditables ?

Les paragraphes qui suivent apportent des éléments de réflexions et de des pistes de solutions, mais ils n'ont pas la prétention de fournir toutes les recommandations et solutions indispensables. Ce serait l'objet d'un tutoriel complet !<sup>7</sup>

## **Qualité et intégrité des données à caractère personnel**

La qualité des processus, en particulier des processus d'identification des personnes physiques, est fondamentale pour la confiance et la fiabilité du système dans son ensemble. Que ce soit de façon purement administrative, lors de l'accueil par l'établissement de soins, lors de l'arrivée pour un séjour d'hospitalisation, que ce soit pour des raisons purement médicales, lors du transfert d'un patient d'un service de soins à un autre, d'une prise en charge avant des soins spécifiques ou pour une opération chirurgicale donnée.

L'intégrité, donc la qualité, des données d'identification est de façon analogue fondamentale et même plus en ce qu'elles permettent au processus d'identification d'être d'un bon niveau de qualité. Une mauvaise identification administrative peut rapidement avoir des conséquences dramatiques, que ce soit en raison de synonymie (enregistrer les informations de l'assuré social dont dépend le patient, au lieu de fournir les informations concernant le patient lui-même, lorsque celui-ci est un ayant droit de l'assuré), ou pour des raisons d'homonymie (enregistrer les informations du patient sur la base d'un séjour d'hospitalisation antérieur d'un autre patient homonyme).

La qualité du processus et l'intégrité des données, surtout en ce qui concerne l'identification des personnes, sont essentiels au bon fonctionnement de l'établissement de soins.

### **Le débat de mots**

L'intégrité des données est souvent confondue avec leur précision et leur exactitude ? Ces notions participent effectivement de l'intégrité des données, mais ne doit-on pas plutôt se poser la question de quand, comment, qui et par qui ces données ont pu être générées et maintenues. Ceci pour apporter toute la confiance nécessaire dans un système d'information sensible, au lieu d'essayer d'atteindre la meilleure précision ou la donnée la plus exacte au risque d'avoir trop de détails sur une donnée déjà devenue obsolète ?

De même, la qualité du système est souvent confondue avec sa fiabilité. Encore faut-il que le système, même s'il est parfaitement fiable, ait été bien conçu c'est-à-dire qu'il prenne en compte les exigences fonctionnelles et les contraintes opératoire auxquelles il doit répondre : un processus très fiable d'identification des personnes ne sera que peu utile si ses conditions de déclenchement ne sont jamais remplies.

<sup>7</sup> Pour plus de détails et une meilleure compréhension, se référer à FD S 97-560, le fascicule de document d'AFNOR qui parcourt exhaustivement, et illustre par divers exemples, toutes les notions et techniques relatives à l'anonymisation.

## **Confidentialité(s) des données à caractère personnel**

Dans un environnement manipulant des données à caractère personnel, la distinction entre préserver la confidentialité-discrétion et respecter la confidentialité-séclusion devient une question-clé de sécurité.

Voici quelques axes de réflexions et pistes de solutions pour mieux appréhender toute la dimension de cette distinction basique mais essentielle.

### **Confidentialité-Discrétion (au sens de « secrecy »)**

- *Lever la discrétion* : la discrétion est une forme de confidentialité qui pourra toujours être levée si les conditions l'autorise : que ce soit techniquement en faisant appel à des algorithmes cryptographiques réversibles ;
- *Cryptographie symétrique ou asymétrique* : sans vouloir faire un cours de base en cryptographie on peut préciser ici que deux types de fonctions cryptographiques sont couramment utilisés pour mettre en œuvre des outils de confidentialité :
  - les fonctions de chiffrement symétrique ou « à clé secrète ». La clé de chiffrement est maintenue secrète entre l'émetteur du message confidentiel chiffré ; le récepteur de ce message chiffré il pourra le déchiffrer avec la même clé ;
  - les fonctions de chiffrement asymétrique ou « à clé publique ». L'équivalent de la clé secrète précédente est cette fois un bi-clé (couple de clés, l'une privée l'autre publique, corrélées mathématiquement), l'une sert dans l'algorithme de chiffrement et l'autre dans celui de déchiffrement ; selon que l'on se sert de la clé privée pour chiffrer puis de la clé publique pour déchiffrer ou, inversement, de la publique pour chiffrer et de la clé privée pour déchiffrer, on parlera de signature ou, inversement, de chiffrement : dans les deux cas il y a réversibilité en utilisant la clé corrélée à celle qui avait servi à protéger.

Dans les deux cas (symétrique ou asymétrique), il y a, au moins techniquement, une solution pour « déprotéger » ce qui a été précédemment protégé. On pourra toujours prétendre que du point de vue du protocole, de l'organisation au sein du service ou de l'entreprise, ou que, par séparation des pouvoirs, il n'est en pratique pas possible de lever la discrétion. Cependant, déchiffrer des identifiants nominatifs remplacés, pour des raisons de protection des données personnelles, par des données chiffrées restera toujours théoriquement possible, donc de médiocre confiance ;

- *Fragmentation/défragmentation* : la fragmentation-dissémination de fichiers permet de garantir la confidentialité des données éclatées en autant de fragments que nécessaire pour assurer un taux de dispersion optimal ; il faut pour cela associer la fragmentation à la dissémination spatio-temporelle, voire à la redondance par répllication des fragments ou autre technique permettant le recouvrement des données d'origine. L'algorithme de fragmentation a pour but de protéger en confidentialité mais sa spécification permet la reconstitution du fichier en le « défragmentant ».

Ainsi, dans tous ces cas, la confidentialité est maintenue jusqu'à ce que la discrétion soit levée éventuellement mais légitimement, par déchiffrement, par défragmentation ou par toute technique analogue. Ces techniques n'ont pas pour but de faire disparaître les noms ou données à caractère personnel, mais seulement d'en restreindre l'accès en lecture, donc l'usage abusif.

Ces techniques réversibles sont applicables lors d'échanges électroniques, pour l'archivage de fichiers, pour la consultation de bases de données en temps réel ; elles ne se conçoivent que dans l'optique de systèmes d'information mis directement au service des usagers. Les noms, coordonnées, profils, caractéristiques ne figurent dans de tels systèmes que pour la finalité des traitements, comme le rappelle la CNIL. En aucun cas, ces données à caractère personnel, compte tenu des obligations d'information, des droits de rectification, droits à l'oubli, etc., ne doivent servir à d'autres finalités. Mélanger les genres serait préjudiciable pour le respect de la vie privée ; d'où l'utilité de la distinction avec la séclusion.

### **Confidentialité-Séclusion (au sens de « privacy »)**

- *Interdire l'indiscrétion* : les techniques de confidentialité-séclusion doivent permettre de s'opposer à toute forme d'indiscrétion, électronique en l'occurrence, que ce soit directement (fonctions à sens unique) ou indirectement (notions d'inférences) ;

- *Cryptographie à sens unique* : une partie de la cryptographie consiste à mettre en œuvre des algorithmes impliquant une certaine perte d'information de manière à ne pas pouvoir faire l'équivalent d'un déchiffrement comme indiqué dans le chapitre précédent ; en effet, selon la théorie de Shannon, on peut démontrer qu'une certaine perte d'information est nécessaire pour rendre irréversible la transformation de certaines données : classiquement on appelle ce type d'algorithme des fonctions dites « de condensation, hachage ou scellement », à ne pas confondre avec les fonctions de compression/décompression<sup>8</sup>.
- *Segmentation* : cloisonnement ou segmentation de sphères de connaissance, annuaires de nommage même anonymisés des individus figurant dans des bases de données sensibles (base de trajectoires de soins, pathologies avérées, prestations sociales,...) ; la segmentation est alors l'homologue de la fragmentation sans aucune technique duale de reconstruction ; dans le respect de la finalité du traitement, la segmentation peut interdire de lever la discrétion ; elle empêche de faire la corrélation entre des faits ou des données qui permettraient de ré-identifier illégitimement les individus statistiques ou qui permettraient de déduire des données sensibles qui ne figurent pas dans la base de données considérée ;
- *Intermédiation* : les australiens l'ont d'abord appelée '*DMA-Data Matching Agencies*', correspond à une « déssegmentation » à la différence près qu'elle doit être spécifiée à l'avance pour être déclarée et légitimée et pour permettre de garder le chemin des segmentations appliquées successivement, de manière à pouvoir reconstruire les corrélations volontairement détruites par la segmentation : sorte de CNIL électronique d'autorisation légale et éthique d'intermédiation entre différents fichiers sensibles.

Dans tous ces exemples, on apportera la preuve, et donc l'auditabilité correspondante, que le nécessaire a été mis en œuvre pour garantir la vie privée des individus, en maintenant la meilleure séclusion possible des données électroniques individuelles, comme l'illustrent les différents concepts et outils pour la séclusion présentés ci après.

## Outils pour la séclusion

### **Anonymat / Anonymie / Anonymité**

Il s'agit là de synonymes en français courant (anonymat) ou en vieux français (anonymie, anonymité) d'un état concernant une donnée ou une information. Il s'agit d'un état de fait et en informatique il faut pouvoir parvenir à cet état de fait : c'est ce que l'on appelle plus généralement l'anonymisation... et autres techniques connexes.

### **Anonymisation / Pseudonymisation**

L'anonymisation et ses diverses variantes, dont l'occultation des noms (éphémère) ou encore la pseudonymisation des identifiants (plus universelle), est une véritable démarche qui inclut une analyse, ou approche, servant un objectif global de respect de la vie privée. Comme indiqué, par la suite, au travers d'un enchaînement de questions pertinentes à se poser (besoins d'anonymat, objectifs d'anonymisation, exigences d'anonymisation), une telle démarche sert à construire la solution d'anonymisation *ad hoc* pour une configuration donnée.

### **Besoins / Objectifs / Exigences**

Les besoins d'anonymisation pourraient presque être multipliés à l'infini, tellement il y a de contextes juridiques, organisationnels ou techniques à prendre en compte : c'est bien souvent la combinaison des réponses à quelques bonnes questions qui permettra alors de cerner le réel besoin : besoin statistique, vision macroscopique ou nécessité microscopique d'entrer dans les détails de données individuelles.

L'objectif, ou finalité du traitement en termes exprimés par la CNIL, contribue à définir quel est le besoin. On peut, selon le FD S 97-560, retenir trois familles d'objectifs : anonymisation réversible (ce qui est un abus de langage, car correspondant plus à de la discrétion provisoire qu'à de la séclusion

<sup>8</sup> Les fonctions de compression s'appuient, elles aussi, sur la théorie de l'information en exploitant la redondance du langage pour supprimer puis restituer les éléments redondants ou superflus lors de la compression puis décompression.

définitive), anonymisation irréversible (dans le vrai sens du terme anonymisation) ou anonymisation inversible (sorte d'intermédiaire entre le réversible et l'irréversible).

Les exigences environnementales permettent de compléter l'analyse de besoins. Elles donnent une image fiable de ce que le responsable de la mise en place d'une procédure d'anonymisation est en droit d'attendre. On parlera souvent d'exigence de robustesse, que ce soit robustesse à la réversion non autorisée des données anonymes en données (re)nominatives, mais aussi robustesse face à des attaques à base de techniques d'inférence pour déduire, induire des informations confidentielles ou nominatives qui ne figuraient pourtant pas à l'origine dans la base de données manipulée.

### **Notions de réversibilité : réversible / inversible / irréversible**

Trois formes de réversibilités et donc trois familles d'anonymisation ont pu être identifiées :

- *Réversibilité* : possibilité de remonter, depuis les données anonymes ou anonymisées, jusqu'aux données nominatives originelles ; cela peut être envisageable et légitime dans certains cas bien précis, mais mieux vaut éviter d'appeler cela de l'anonymisation pour éviter toute confusion et plutôt parler chiffrement, car telle est la technique qui se cache derrière ;
- *Irréversibilité* : c'est le cas de la réelle anonymisation car décidée et irréversible, comme la séclusion est délibérée et irrémédiable ; une fois remplacé par des identifiants anonymes, les identifiants nominatifs originels ne sont plus recouvrables, de même que remplacées par des pseudonymes les identités ne doivent plus être retrouvables. Cependant, avec les techniques d'attaque par inférence, les pseudonymes s'ils sont trop universellement utilisés risquent de permettre la découverte d'identités mal cachées, comme on l'explique ci-après ;
- *Inversibilité* : il s'agit là d'un cas mixte entre réversibilité et irréversibilité, c'est-à-dire entre le '*techniquement ou cryptographiquement irréversible*' et le '*organisationnellement et juridiquement réversible*' ; dans ce cas, il faut faire appel à une instance légitime, un tiers de confiance de levée d'anonymat, pour respecter et faire respecter l'intimité électronique de la vie privée des individus concernés. Par analogie, rappelons qu'un représentant de l'Ordre, que ce soit des avocats, des médecins ou des notaires doit être présent lors d'une perquisition, pour faire respect la déontologie et l'éthique de l'Ordre en question, dans l'intérêt du citoyen.

### **Notions de robustesse : à la réversion / à l'inférence**

Nous retiendrons deux types de robustesses.

- *Robustesse à la réversion* : contrairement à la réversibilité la réversion de données n'est pas une capacité souhaitée mais une défaillance face à des risques de perte d'anonymat :
  - ainsi, la réversion peut être directe par des attaques illicites pour retrouver des noms profitant de la faiblesse ou du manque de robustesse de, par exemple, un algorithme cryptographique reconnu pour avoir des failles (fonction à sens unique faillible) ;
  - ou bien, la réversion peut être indirecte si elle profite d'une organisation fragile pour, de façon procédurale, permettre de rétablir la correspondance entre les identifiants anonymisés et les identifiants nominatifs originels et donc violer l'anonymat ;
- *Robustesse à l'inférence* : dérivée de la réversion, l'inférence est une notion qui consiste à dévoiler des informations confidentielles (noms désanonymisés, ou données sensibles) à partir d'autres informations moins confidentielles ou sensibles. Il en existe plusieurs variantes :
  - *L'inférence déductive ou déduction* est la forme la plus connue d'inférence et consiste par la logique souvent booléenne (*valeurs* : oui, non ; *opérateurs* : et, ou) à engendrer des informations simples mais non encore présentes dans la base de données ;
  - *L'inférence inductive ou induction* s'apparente souvent à des raisonnements de type loi des grands nombres sans forcément l'appliquer sur de grandes échelles ; cela consiste, par exemple, à induire qui tel patient est très certainement atteint de telle pathologie compte tenu du fait qu'il lui est prescrit tels médicaments comme il est d'usage pour cette pathologie ;

- *L'inférence abductive* ou *abduction*<sup>9</sup> correspond au fait d'extrapoler une situation (une vue partielle de la situation informatique) vers une situation logiquement plus stable, à condition d'ajouter un précepte ou une hypothèse parfois 'tirée par les cheveux' mais finalement fondée : « et s'il avait un cancer, cela expliquerait pourquoi il s'absente parfois d'un Conseil des Ministres pour se rendre du côté de Villejuif... !!! » ;
- *L'inférence adductive* ou *adduction*<sup>10</sup>, inverse de l'abduction, permet d'interpréter une situation externe au système informationnel, pour la rapprocher d'une réalité informatique : « il a été vu en consultation à Villejuif et de tous les individus statistiques présents dans la base, c'est le seul : il est donc bien le numéro XXXX ».

### **Notions de chaînage : spatial / temporel et nul / partiel / total**

Une autre notion importante, en matière d'anonymisation, est le chaînage d'informations anonymes associées à un même individu dit statistique : épisodes de soins, prestations sociales, prescriptions, symptômes, pathologies, ... pour ne prendre que des illustrations issues de la santé ou du social. Ce besoin de chaînage ouvre les risques d'inférence du plus basique (déduction et induction) au plus complexe (abduction et adduction), le chaînage pouvant être spatial / temporel, nul, partiel ou total...

Le chaînage est à la fois un besoin légitime pour mener à bien des travaux et étude, fondés et un risque. Ce risque est encouru dès lors qu'il y a déviance de comportement autour de l'utilisation d'outils informatiques qui permettent de rassembler une grande quantité d'informations privatives sur un individu donné : risque d'atteinte à l'intimité électronique des personnes auxquelles elles appartiennent.

## **Conclusions**

Les propriétés, décrites dans cet article, sont plus ou moins novatrices dans la réflexion de notre communauté ADELI. Par ailleurs, elles sont plus ou moins bien évoquées, et parfois évacuées, faute de temps ou de ressources motivées pour les développer et les remanier.

Ces propriétés ne sont que des associations ou combinaisons, plus ou moins subtiles, d'une kyrielle de propriétés élémentaires à satisfaire puis de techniques de base à assembler et mettre en œuvre. Mais elles répondent à l'un des soucis récents, mais majeurs, engendrés par les nouvelles technologies de l'information et la communication : le respect de la vie privée et la protection de l'individu, dans une dimension électronique qui devient désormais omniprésente.

*Avis*

par courriel : [gilles.trouessin@ernst-young.fr](mailto:gilles.trouessin@ernst-young.fr)

par téléphone : +33 (0) 6 8255.7406

par la toile : [www.adeli.com](http://www.adeli.com)

par télécopie : +33 (0) 1 5847.1033

par courrier : Ernst & Young Audit (France) - Tour Ernst & Young - 92037 PARIS La Défense Cedex

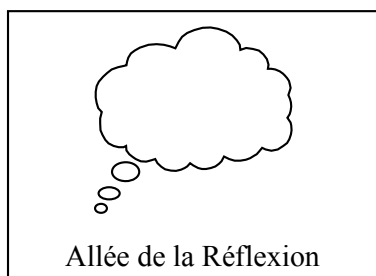
**Gilles Trouessin**

*Vice-président d'ADELI "en charge de l'innovation"  
 Directeur de Mission au sein de 'Ernst & Young Audit'  
 Animateur du GE-SSIS et membre des CN IS et CN SSI  
 Expert au CEN/TC251/WGiii et à l'ISO/TC251/WG4 et 5*

AFNOR/GE-SSIS :	Groupe d'Experts 'Sécurité des Systèmes d'Informations de Santé' d'AFNOR
AFNOR/CN IS :	Commission de Normalisation 'Informations de Santé' d'AFNOR
AFNOR/CN SSI :	Commission de Normalisation 'Sécurité des Systèmes d'Information' d'AFNOR
CEN/TC251/WGiii :	Groupe de Travail 'Security, Safety et Quality' du Comité Technique 'Health Informatics' du CEN
ISO/TC215/WG4 & 5 :	Groupes de Travail 'Security' & 'Health cards' du Comité Technique 'Health Informatics' à l'ISO

<sup>9</sup> Par analogie avec un muscle abducteur qui permet à un membre de s'écarter du plan médian du corps.

<sup>10</sup> Par analogie avec un muscle adducteur qui rapproche un membre ou un doigt du plan médian du corps, ou de la main.



# Une facture d'hôpital à la veuve du donneur !

**Le management du système d'information hospitalier**

*Gérard Ponçon a publié en mars 2000, aux éditions ENSP (École nationale de la santé publique) l'ouvrage « Le management du système d'information hospitalier » sous-titré « La fin de la dictature technologique » dont sont extraites les lignes suivantes.*

*Nous pouvons, bien entendu, étendre ces conclusions tirées dans le milieu médical à d'autres milieux professionnels.*

## Une fiction

Voilà quel pourrait être un gros titre de la presse locale, venant une fois de plus fustiger l'hôpital. L'article pourrait être libellé ainsi :

« Qu'elle n'a pas été l'émotion de Madame X en recevant, le 25 janvier dernier, une facture du Centre hospitalier de la ville, à la suite du prélèvement d'un rein sur le corps de son mari, décédé accidentellement ...

Le Directeur de l'hôpital, manifestement affecté par cette insupportable bévue de ses services, a adressé à la famille du donneur les excuses qu'une telle situation exigeait.

Il a indiqué à notre correspondant qu'un tel incident ne saurait se reproduire dans son établissement et que des directives seraient étudiées pour que toute facture soit systématiquement vérifiée avant expédition. ».

## La réalité n'est sûrement pas loin de cette fiction

À l'évidence, un agent avait connaissance de l'information précisant la nature exceptionnelle de l'intervention, mais non l'agent chargé d'enregistrer les actes de bloc opératoire en vue de facturation, ni l'agent chargé de l'expédition des factures (appelées « titres de recette » dans le langage administratif hospitalier). Il s'agit donc d'un problème de système d'information. Qui le contestera ?

Nous savons que rien de ce qui se passe à l'hôpital n'est étranger au système d'information. Nous savons aussi que celui-ci a beaucoup de difficultés à identifier l'information nécessaire à une tâche donnée et à la rendre disponible à l'endroit qui convient pour une bonne décision. Alors que faire ?

Dans notre exemple, le chef d'établissement demandera-t-il, sans aucun doute, que le programme informatique soit modifié. Mais, se posera alors le problème de la connaissance exhaustive des situations qui pourraient se présenter ; exercice impossible ...

Cela nous permet, en conclusion, d'exposer deux convictions que nous aimerions partager avec les responsables de système d'information et qui devraient éclairer toutes réflexions et études.

## Première conviction : le système d'information doit être centré sur le patient

S'agirait-il d'une simple commodité facilitant l'organisation du système d'information en vue d'une facturation exhaustive, du partage efficace d'un dossier, de la recherche sécurisée des antécédents hospitaliers du patient ?

Ne serait-ce que cette simple commodité ? L'établissement en serait déjà mieux géré.

Loin de la simple formule, servant d'ailleurs d'alibi, dans bien des cas, bâtir le système d'information autour du patient conduit à élargir la réflexion. En particulier, cette approche permet d'aborder le

champ de la qualité qui se définit comme la « capacité d'un service à répondre à l'attente d'un client et à lui donner satisfaction ».

La question fondamentale qu'il faut poser en abordant l'étude de l'évolution du système d'information est la suivante : un système d'information de qualité peut-il réellement contribuer à la satisfaction des besoins du patient et de son entourage ?

Il le peut, si « centrer sur le patient » veut dire :

- que chaque agent s'assure de la qualité de toute donnée introduite dans le système d'information et qu'il est prêt à certifier qu'il a fait tout ce qu'il devait faire pour qu'elle soit de qualité ;
- que, lors de chaque étude d'évolution du système d'information, on s'assure que le besoin exprimé est bien compris et convenablement mis en forme.

## **Deuxième conviction : le système d'information est en mesure de préserver l'humanité de l'hôpital**

Avoir cette conviction - serait-ce une utopie ? - conduit à inventer les indicateurs que le système d'information gèrera pour alerter ses utilisateurs. Il s'agit, bien sûr, de savoir que le patient est décédé et qu'il a fait don de son corps ; ainsi la facture ne sera pas envoyée à sa veuve.

Mais, surtout, il s'agit de la volonté très déterminée de l'ensemble des utilisateurs de partager l'information en s'interdisant toute action visant à renforcer la propriété exclusive de cette information. Et, lorsque l'information ne peut être partagée pour d'évidentes raisons de confidentialité, il faut qu'un indicateur alerte l'agent sur la disponibilité d'une telle information qu'il devra rechercher auprès d'un de ses collègues.

Par exemple, une information détenue par une assistante sociale est très protégée ; toutefois, il faut que les agents autorisés sachent que cette information existe afin de la lui demander, s'ils en ont besoin.

En fin de compte, tout peut se résumer en une simple phrase : « L'humain doit primer ». Le système d'information a sa place dans cette affirmation qui néanmoins le dépasse.

## **Voilà la grande utopie...**

Au terme de cet article, qu'il nous soit pardonné de mêler Victor Hugo<sup>1</sup> à notre recherche et de rapprocher dans une même quête l'organisateur et le poète :

*« Le poète en des jours impies  
Vient préparer des jours meilleurs.  
Il est l'homme des utopies ;  
Les pieds ici, les yeux ailleurs »*

**Gérard Ponçon**  
**Assistance publique – Hôpitaux de Marseille**  
**auteur de l'ouvrage**  
**« Le management du système d'information hospitalier**  
**Fin de la dictature technologique »**

---

<sup>1</sup> In « poème « Fonction du poète » » dans le recueil « les rayons et les ombres »

## Quelques extraits de la préface de l'ouvrage

Depuis le rapport de l'IGAS<sup>2</sup> sur l'état de l'informatique hospitalière en 1995, les établissements publics de santé, dans leur majorité, n'ont guère progressé et peinent à mettre en œuvre les « nouvelles technologies de l'information et de la communication » dont le monde entier vante les mérites réels ou supposés.

Les systèmes d'information hospitaliers restent, pour la plupart, à construire mais les chefs d'établissement ne perçoivent pas toujours l'importance fonctionnelle et stratégique de tels chantiers. J'en veux pour preuve l'échec récent d'un programme de formation au management des systèmes d'information destiné aux directeurs d'hôpital, conçu et coproduit par l'ENSP (École nationale de la santé publique) et le CNEH, sous le haut patronage de la direction des hôpitaux : après quatre mois de publicité, seuls, trois chefs d'établissement s'étaient inscrits...

Le sujet impressionne-t-il ? Fait-il peur ? Pourtant les directeurs, aujourd'hui en poste, savent parfaitement affronter des difficultés et des contraintes bien plus angoissantes.

Je pense que ce sujet est méconnu pour avoir été trop longtemps abandonné à des spécialistes au langage hermétique ou à des bidouilleurs géniaux et incompris. Toute tentative de démystification doit donc être saluée et soutenue, car aujourd'hui le management des systèmes d'information est aussi indispensable à la pérennité d'un hôpital que le management des hommes.

Pour toutes ces raisons, le livre de Gérard Ponçon arrive parfaitement à point. De plus, il cumule deux qualités qui justifient largement sa publication par l'ENSP.

Tout d'abord, *c'est un livre de management*, il s'adresse aux personnels de direction des établissements de santé publics et privés. Ce n'est pas un précis d'informatique. Son objectif est bien d'améliorer le recueil, la circulation et l'usage des millions d'informations qui circulent dans nos hôpitaux, et cet objectif est soutenu par la volonté permanente de parfaire la prise en charge des patients qui nous font confiance. Le management des systèmes d'information donne, aux responsables hospitaliers, l'occasion de réfléchir sur l'organisation des différents processus de production à fort contenu informationnel dans l'hôpital et de les faire évoluer positivement.

Ensuite, *c'est un ouvrage pédagogique* et d'utilisation immédiate : des définitions de la première partie jusqu'aux conseils pratiques en annexe, le lecteur suit avec aisance et profit le cheminement de la pensée de l'auteur. Ce souci pédagogique, Gérard Ponçon l'a développé dans de nombreux centres hospitaliers où il a réalisé des audits des systèmes d'information et accompagné la mise en œuvre de schémas directeurs. Le lecteur retrouvera dans son livre, quasiment à chaque page, son souci d'associer à la réorganisation des systèmes d'information tous les acteurs et opérateurs de l'hôpital quitte à bousculer les hiérarchies.

Mais, Gérard Ponçon a également fait profiter de son expérience les stagiaires de l'ENSP en formation initiale ou continue. Durant de nombreuses années, au contact parfois abrasif de nos élèves, son discours s'est poli, son enseignement s'est épuré.

Son ouvrage est donc le fruit de cette féconde confrontation avec des étudiants « novices » et des hospitaliers désireux de surmonter leurs difficultés quotidiennes. Il est le résultat d'une réflexion théorique mise à l'épreuve des faits, enrichie par l'action et validée par les usagers. Souhaitons que sa lecture ouvre de nouveaux champs de réflexion et d'actions constructives au sein des hôpitaux.

**Philippe PEYRET**  
**Directeur d'hôpital**  
**Professeur de gestion hospitalière à l'ENSP**

---

<sup>2</sup> Inspection générale des affaires sociales





# Des moutons et des robots

## Notes de lecture

*Nous vous proposons cette brève note de lecture de l'ouvrage, publié sous ce titre, par les presses polytechniques et universitaires romandes –collection META. Cet ouvrage est issu d'une thèse soutenue par Pierre Arnaud, en 1999, et primée par la Société Université et Recherche.*

*Dans la LETTRE n° 37 d'octobre 1999, nous vous avons présenté l'ouvrage « Idées nettes sur la logique floue » rédigé par Jelena Godjevac. Le présent ouvrage se veut en être un prolongement. Le lien entre les deux ouvrages s'effectue par le robot Khepera, présent dans les deux ouvrages.*

*Il n'est évidemment pas question de résumer cet ouvrage en quelques pages ; nous nous contenterons d'en évoquer le sommaire pour suggérer à ceux d'entre vous qui seront intéressés par le sujet de se plonger dans le texte complet.*

## Pourquoi ce titre ?

L'observation d'une colonne de chenilles processionnaires a déclenché, assez récemment, une idée fondatrice chez les architectes de la robotique. Ils s'inspirent désormais du comportement des sociétés animales pour modéliser ce qu'on appelle l'« intelligence ».

## Qu'est ce que l'intelligence ?

Initialement, le mot « intelligence » désignait la faculté de comprendre. Son sens s'est enrichi au fil de l'usage et aujourd'hui, l'intelligence apparaît comme un paradigme à multiples facettes dont nous extrayons les suivantes :

- ajuster son comportement en fonction des conditions changeantes de l'environnement ;
- une capacité d'adaptation à des problèmes nouveaux et à des conditions de vie nouvelle ;
- une analyse du mécanisme du traitement de l'information par le cerveau humain.

L'intelligence s'articule autour de cinq types de composants :

- les métacomposants, processus de niveau supérieur, dirigeant la résolution générale du problème ;
- les composants de performance, utilisés pour la résolution de chaque problème particulier ;
- les composants d'acquisition, processus d'apprentissage ;
- les composants de rétention, processus de restitution des informations mémorisées ;
- les composants de transfert, processus de généralisation.

L'auteur étudie les différentes formes d'intelligence naturelle et effectue un rapide historique des péripéties de l'intelligence artificielle, au fil de l'évolution de l'informatique.

## Les robots dans l'histoire

Depuis l'antiquité, les hommes ont toujours rêvé de créer des êtres artificiels à leur image, susceptibles de s'acquitter des tâches considérées comme les moins nobles.

- Pygmalion, sculpteur de Chypre, avait créé une statue de Galatée, à laquelle Aphrodite avait insufflé la vie.
- Au XVI<sup>e</sup> siècle circule la légende de Golem (dite du rabbin de Prague). Une statue de petite taille agissait comme un serviteur docile. On pouvait l'animer en inscrivant le mot hébreu EMET (vérité) et de le mettre au repos en supprimant le E (MET signifie mort en hébreu).
- En 1818, un roman de Mary Shelley a créé le célèbre Frankenstein par une utilisation de l'énergie électrique.
- En 1920, la pièce de Karel Čapek (*Rossum's Universal Robots*) mettait en scène des robots. Des automates, destinés à faire le travail des hommes et à améliorer leur condition de vie, se rebellent et prennent la place de l'humanité.

Isaac Asimov, en 1942, a émis les trois lois de la robotique

- Un robot ne peut porter atteinte à un être humain ni, restant passif, laisser cet être humain exposé au danger.
- Un robot doit obéir aux ordres donnés par les êtres humains, sauf si de tels ordres sont en contradiction avec la première loi.
- Un robot doit protéger son existence, dans la mesure où cette protection n'est pas en contradiction avec les deux lois précédentes.

La *Machina Speculatrix*, robot analogique développé en 1951 par Walter explore en permanence l'environnement. Il est doté d'un tropisme positif vers les sources lumineuses et d'un tropisme négatif vis-à-vis des sources lumineuses trop intenses, des obstacles et des pentes. Il se reconnaît lui-même, placé devant un miroir, et reconnaît des êtres identiques. Le robot est autonome ; son tropisme le conduit à se diriger vers le nid pour se recharger.

## Les déplacements collectifs

L'ouvrage analyse les différentes organisations collectives d'êtres vivants : troupeau (moutons), volée (martinets), banc (poissons), formation (oiseaux migrateurs), front (criquets), procession (chenilles), essaim (abeilles), groupe sans structure (poussins).

Chaque organisation possède ses propres caractéristiques : directions de déplacement, présence ou non d'un meneur, distances entre les individus, protection contre les agressions, ... et présente, ainsi, des avantages et des inconvénients en fonction des contextes qui lui sont imposés.

### ***Intérêt du déplacement collectif de robots***

L'auteur donne des cas d'emploi qui appellent la coordination d'un ensemble de robots :

- exploration de l'environnement (déménagement par exemple) ;
- collaboration pour le transport d'objets lourds et volumineux ;
- répartition des rôles au sein du groupe pour le partage d'informations.

### ***Programmation des collectifs de robots***

L'étude des déplacements des groupes d'animaux permet d'orienter les recherches sur les déplacements collectifs de robots.

On implémente ainsi quelques comportements simples :

- évitement d'obstacles, poursuite, agrégation, dispersion, retour.

On implémente des dispositifs de maintien de la disposition des individus du groupe :

- par rapport au centre du groupe, par rapport au meneur, par rapport au voisin.

## Techniques de localisation

L'auteur décrit les principales techniques actuellement utilisables pour matérialiser les concepts nécessaires aux déplacements des robots :

- capteurs ;
- mesures de distance et de détection d'obstacles ;
- mesures de position et de déplacement ;
- mesures des grandeurs internes (par exemple, niveau de la réserve d'énergie).

## Architecture à fusion d'actions, généralisée

L'architecture du robot régit l'articulation et l'imbrication des différentes fonctions jouées par le robot (détection, modélisation, planification, action).

Après la présentation des principales architectures :

- architecture à subsomption ;
- architecture à sélection d'actions ;
- architecture orientée schémas ;

L'auteur présente une notation qui permet de traiter les différentes architectures, en les unifiant dans un formalisme unique qui devient celui de l'architecture dite à fusion d'actions, généralisée.

Cette architecture offre un système de coordination de comportements élémentaires, basé sur un réseau de nœuds (de type : inhibition, suppression, augmentation).

Ce chapitre est suivi de la construction d'un contrôleur basé sur l'architecture à fusion d'actions généralisée. Cette étude montre les avantages de cette architecture par rapport aux autres architectures réactives.

## Les robots Khepera

L'ouvrage contient une description technique détaillée du robot mobile Khepera et analyse les retours d'expériences menées avec ces groupes de robots mobiles Khepera.

L'ouvrage se termine par l'énumération de 300 références bibliographiques.

## En conclusion

Cet ouvrage, bien structuré et clairement écrit, se prête à plusieurs niveaux de lecture.

Pour les profanes, c'est une bonne introduction à la découverte des groupes de robots mobiles.

La conception de tels robots implique la coordination de spécialistes de différentes disciplines : mathématiques, informatique, physique, biologie, philosophie, ...

Chaque spécialiste pourra vérifier la bonne prise en compte des concepts de sa discipline et comprendre leur intégration avec ceux des disciplines complémentaires.

*Alain Coulon*  
*Secrétaire d'ADELI*



# Problème de logique

*Un petit casse-tête*

*À l'approche des congés d'été, nous vous soumettons ce petit jeu pour meubler une sieste.*

## Distribution des rôles

Cinq amis : Alain, Camille, Jean, Pierre et Robert, se rencontrent, autour d'un bon repas. Chacun d'eux :

- habite une région ;
- possède un animal ;
- pratique un sport ;
- a une couleur préférée.

Les 5 régions : Aquitaine, Bretagne, Corse, Île de France, Picardie.

Les 5 animaux : chien, chat, cheval, vache et lapin.

Les 5 sports : pêche, chasse, ski, natation et boules.

Les 5 couleurs : vert, jaune, rouge, bleu et gris.

## Observations relevées au cours de la réunion

Le propriétaire du chat fait de la natation.

Le chien et la vache ont des maîtres qui habitent en Aquitaine et en Bretagne.

Alain est à droite du cheval et à gauche de la Corse.

Pierre habite en Picardie.

Robert, qui est habillé en rouge, fait du ski.

Pierre et Camille pratiquent, l'un la pêche, l'autre la natation.

Le chasseur aime beaucoup aller chez son voisin tirer le lapin.

Le jaune et le bleu encadrent le rouge.

Le vert est séparé de l'Île de France par le nageur.

Jean est à gauche de la Bretagne.

## Questions

Qui aime le gris ?

Qui joue aux boules ?

Qui habite l'Aquitaine ?

*Retrouvé par Alain Coulon  
Solution au prochain numéro*

# ADELI

Association pour la maîtrise des systèmes d'information

## Adhésion Entreprise 2001

### Coordonnées de l'entreprise

Organisme	_____
Adresse	_____ _____ _____
Téléphone	_____ Site Web _____

### Coordonnées du représentant de l'entreprise adhérente

Nom - Prénom	_____
Adresse (si différente)	_____ _____ _____
Téléphone	_____ Portable _____
Fax	_____
Portable	_____
Adresse électronique	_____ @ _____

Les entreprises adhérentes reçoivent,  systématiquement et gratuitement , toutes les publications de l'association émises au cours de l'année, ainsi que l'annuaire des adhérents.

### Montant de la cotisation 2001

**1.200 FRF ou 182,94 EUR**

Cadre réservé à ADELI
Règlement
Nature : _____
n° pièce : _____
Numéro d'adhérent : _____

Le ___ / ___ / ____ à _____
-----------------------------

Cachet de l'entreprise et signature